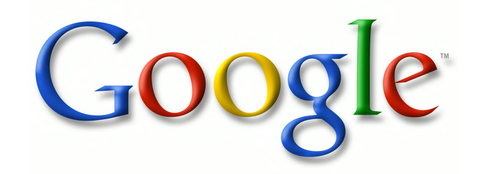
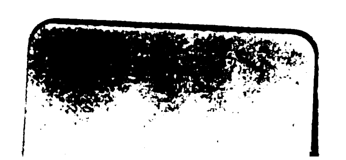




VORLESUNGEN ÜBER ZAHLENTHEORIE

EINFÜHRUNG IN DIE THEORIE
DER ALGEBRAISCHEN ZAHLKÖRPER

VON

DR. J. SOMMER

PROFESSOR AN DER TECHN. HOCHSCHULE IN DANZIG

MIT 4 FIGUREN IM TEXT

LEIPZIG UND BERLIN
DRUCK UND VERLAG VON B. G. TEUBNER
1907

Vorwort.

Seitdem Gauß die Arithmetik durch Aufnahme der komplexen Zahlen $a + b\sqrt{-1}$ erweitert hat, ist eine großartige Theorie der allgemeinen algebraischen Zahlen entstanden, deren Entwicklung vor allem an die Namen Kummer, Dirichlet, Dedekind, Kronecker und einiger rühmlichst bekannten neueren Mathematiker sich knüpft. Mehrfach hat diese Theorie ihr Aussehen stark verändert, und wir besitzen von den berufensten Seiten: Dedekind, Hilbert und Kronecker-Hensel, sowie neuerdings von Herrn Bachmann zusammenfassende Werke, welche den Stoff von verschiedenen Gesichtspunkten aus auffassen. Jedes dieser Werke bedeutet nicht bloß in bezug auf den Inhalt, sondern auch in Anbetracht der formalen Abrundung der ganzen Darstellung einen sehr wesentlichen Fortschritt für die allgemeine Zahlentheorie.

Da dieselben alle den allgemeinen Fall der Theorie umfassen und für Anfänger schwierig zu lesen sind, so schien mir eine Darstellung nützlich zu sein, welche auf möglichst elementare Weise in ihre Probleme und Tatsachen einführt. Dieser Zweck wird von selbst durch eine spezielle Behandlung der einfachsten, quadratischen und kubischen Zahlkörper erreicht.

---

1) P. G. Lejeune-Dirichlet, Vorlesungen über Zahlentheorie. 4. Aufl. Braunschweig 1894. Supplement XI.

2) D. Hilbert, Die Theorie der algebraischen Zahlkörper. Bericht, erstattet der deutschen Mathematiker-Vereinigung. Jahresber. der deutsch. Math.-Vereinigung. 4. Bd. Berlin 1894. Ich zitiere dieses Werk im folgenden kurz als Zahlber. oder Bericht.

3) L. Kronecker, Vorlesungen über Zahlentheorie, herausg. von K. Hensel. 1. Band. Berlin 1901.

4) P. Bachmann, Zahlentheorie. 5. Band; Allgemeine Arithmetik der Zahlenkörper. Leipzig 1905.

An diese Stelle gehören außerdem mehrere Kapitel aus:

H. Minkowski, Geometrie der Zahlen. 1. Lief. Leipzig 1896.

Zum Studium des vorliegenden Buches sind nur wenige Vorkenntnisse aus der Algebra notwendig. Ich habe gesucht, überall mit den einfachsten Methoden zum Ziele zu gelangen, und habe mich überhaupt derjenigen Behandlung der Theorie angeschlossen, die mir als die einfachste erscheint und welche man in den Arbeiten von Hurwitz, Hilbert und Minkowski niedergelegt findet. Dieselbe wurde mir noch näher gebracht durch eine Vorlesung vom Winter 1897/98, in welcher Herr Hilbert u. a. die Elemente der Lehre des quadratischen Zahlkörpers mit Anwendungen auf das „letzte Theorem" von Fermat behandelt hat. Seine voraussetzungslose, einfache und klare Darstellung ist mir stets ein Vorbild bei meiner Arbeit gewesen.

Bei den Korrekturen bin ich durch Herrn Dr. A. Timpe in Danzig und Herrn Privatdozenten Dr. R. Fueter in Marburg unterstützt worden. Dank der wertvollen Hilfe des letzteren konnte ich in der Darstellung einiger Beweise und in manchen Einzelheiten wichtige Verbesserungen anbringen. Ich bin den beiden genannten Herren zu herzlichem Danke verpflichtet. Besonders aber schulde ich Herrn Geheimrat Hilbert den größten Dank für die Aufmunterung in meiner Arbeit und für viele Förderung im mündlichen Verkehr. Er hatte außerdem die Freundlichkeit, mir für einen wesentlichen Punkt in meiner Darstellung (Nr. 15) das Manuskript einer früheren Vorlesung zur Verfügung zu stellen.

Langfuhr, Dezember 1906.

J. Sommer.

Inhaltsverzeichnis.

Erster Abschnitt.

Einleitung.

Zweiter Abschnitt.

Der quadratische Zahlkörper.

Dritter Abschnitt.

Seite

Anwendungen der Theorie des quadratischen Zahlkörpers.

Vierter Abschnitt.

Zahlkörper dritten Grades.

Fünfter Abschnitt.

Relativkörper.

Erster Abschnitt.

Einleitung.

Die Theorie des quadratischen Zahlkörpers, welche hauptsächlich im folgenden zu entwickeln ist, will die Sätze über die ganzen natürlichen Zahlen auf allgemeinere Zahlen ausdehnen. Diese Verallgemeinerung ist nicht bloß um ihrer selbst willen interessant, es wird sich vielmehr zeigen, daß manche sonst schwer beweisbare Tatsachen der elementaren „rationalen" Zahlentheorie als einfache Folgerungen der allgemeinen Theorie erscheinen. Die wichtigsten Sätze der elementaren Theorie, die in der allgemeinen Theorie wieder zur Besprechung kommen, wollen wir in gedrängter Form hier anführen, um durch die Gegenüberstellung der Theoreme aus beiden Gebieten das Verständnis der allgemeineren Theorie zu erleichtern.[1])

---

1) Wegen aller Einzelheiten sei auf die vorhandenen ausgezeichneten Lehrbücher verwiesen, unter denen ich z. B. nenne:

P. G. Lejeune Dirichlet, Vorles. über Zahlentheorie. Herausgeg. von Dedekind. 4. Aufl. 1894.

P. L. Tschebyscheff, Theorie der Kongruenzen. Deutsch herausgeg. von H. Schapira. Berlin 1889.

P. Bachmann, Zahlentheorie. Band I: Elemente der Zahlentheorie. Leipzig 1892.

Ders., Niedere Zahlentheorie. 1. Teil. 1902.

Sehr viele Anregungen beim Studium der Zahlentheorie verdanke ich dem reichhaltigen Bericht von Smith: H. J. St. Smith, Collected mathematical papers. Vol. I. Report on the theory of numbers. 6 parts. p. 38—364. Oxford 1894. Die sechs Teile des Berichtes sind ursprünglich erschienen in den Jahren 1859 bis 1865, Report of the British Association.

Niemand, der sich eingehend mit der Zahlentheorie beschäftigen will, darf das Studium der klassischen Originalwerke von Lagrange, Gauß, Legendre, Dirichlet versäumen:

C. F. Gauß, Disquisitiones arithmeticae. Lips. 1801. Ges. Werke, Bd. I, in deutscher Übersetzung herausgeg. von H. Maser, Berlin 1889.

A. M. Legendre, théorie des nombres, in deutscher Übersetzung nach der 3. Aufl. des Originals herausgeg. von H Maser. 2 Bde. Leipzig 1886.

1. Teilbarkeit der ganzen rationalen Zahlen.

Zunächst treffen wir bezüglich der Bezeichnungen die Festsetzung: die positiven oder negativen rationalen ganzen Zahlen seien durchgängig mit (kleinen) lateinischen Typen $a, b, \ldots$ bezeichnet; insbesondere sollen Primzahlen mit p, q, beliebige Zahlen mit $a, b, c, \ldots$ bezeichnet werden. Dabei heißt wie üblich eine Zahl Primzahl, wenn sie außer durch ± 1 nur durch sich selbst teilbar ist. Die Zahl ± 1 soll im allgemeinen nicht als Primzahl gelten. Zwei Zahlen a und b heißen *teilerfremd* oder *prim zueinander*, wenn es keine Primzahl $p > 1$ gibt, die in a und b zugleich aufgeht.

Der *Fundamentalsatz* der elementaren Zahlentheorie spricht die Tatsache aus, daß jede ganze rationale Zahl sich wesentlich nur auf *eine* Weise in ein Produkt aus Primfaktoren zerlegen läßt, wobei der Zusatz „wesentlich“ bedeuten soll, daß zwischen positiven und negativen Faktoren nicht unterschieden wird.

Der Beweis dieses Satzes stützt sich auf das Euklidische Teilerverfahren, d. i. die Methode zur Bestimmung des gemeinsamen Faktors irgend zweier ganzer rationaler Zahlen. Diese Methode hat auch für viel allgemeinere Untersuchungen Verwendung gefunden, und es ist wichtig, daß man sich das Prinzip derselben am einfachsten Fall ganz klar macht.

Seien a und b zwei ganze rationale (der Einfachheit wegen positive) Zahlen und $a > b$, so kann man die Gleichung ansetzen:

$$a = qb + r_0,$$

wo $b > r_0 \geqq 0$ und r_0 der Rest bei der Division von a durch b ist, während q die ganze Zahl bedeutet, welche angibt, wie oft b in a ganz enthalten ist. Falls $r_0 > 1$, so dividiere man ebenso b durch r_0, so daß

$$b = q_1 r_0 + r_1$$

wird, wo $r_0 > r_1 \geqq 0$ ist, und setze dieses Verfahren fort, indem man r_0 durch r_1 dividiert, usw.; dadurch erhält man ein System von *endlich vielen* Gleichungen:

$$\begin{aligned} a &= qb + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ r_{n-2} &= q_n r_{n-1} + r_n, \end{aligned}$$

da das Divisionsverfahren nach einer endlichen Anzahl $n + 1$ von

Schritten zu einem Rest $r_n = 1$ oder $r_n = 0$ führen muß. Weil $r_0, r_1, r_2, \ldots$ positive ganze Zahlen sind und $r_0 > r_1 > r_2 \ldots$, so muß notwendig $n + 1 < b$ sein. Falls $r_n = 1$ ist, sind die beiden Zahlen a und b teilerfremd. Falls aber $r_n = 0$ und $r_{n-1} > 1$, so haben die beiden Zahlen a und b den gemeinsamen Teiler r_{n-1}, im speziellen Fall, wenn $r_0 = 0$ wäre, so ist b selbst dieser gemeinsame Teiler.

Wenn nämlich $r_n = 0$ ist, geht r_{n-1} in r_{n-2} auf, und da wegen der Gleichung:

$$r_{m-2} = q_m r_{m-1} + r_m$$

r_{n-1} auch in r_{m-2} aufgehen muß, falls es in zwei aufeinanderfolgenden Resten r_{m-1} und r_m aufgeht, so geht r_{n-1} also der Reihe nach in $r_{n-2}, r_{n-3}, \ldots r_1, r_0, b$ und a auf. Zugleich ist $r_{n-1} = t$ der größte gemeinsame Teiler von a und b. Aus der Betrachtung der Divisionsgleichungen von oben nach unten folgt nämlich, daß der größte gemeinsame Faktor irgend zweier aufeinanderfolgender Reste r_{m-2}, r_{m-1}, wegen der Gleichung:

$$r_{m-2} = q_m r_{m-1} + r_m$$

oder

$$r_m = r_{m-2} - q_m r_{m-1},$$

auch in dem folgenden Rest r_m enthalten ist. Der größte gemeinsame Faktor von a und b ist also der Reihe nach auch in $r_0, r_1, \ldots r_{n-1}, r_n$ enthalten.

Wenn $r_n = 0$ ist, so ist r_{n-1} dieser größte gemeinsame Teiler, wenn aber $r_n = 1$ ist, so sind a und b teilerfremd.

Auf Grund dieser Bestimmung läßt sich nun folgender Hilfssatz beweisen:

Hilfssatz. Wenn das Produkt von zwei ganzen Zahlen aa_1 durch eine dritte ganze Zahl b teilbar ist, und es ist a prim zu b, so muß a_1 teilbar sein durch b.

Man schreibt wieder das Divisionsverfahren an für a und b, indem dabei nach der Voraussetzung über a und b die Zahl $r_n = 1$ zu setzen ist. Multipliziert man alle Gleichungen der Reihe nach mit a_1, so daß man das System erhält:

$$aa_1 = qba_1 + r_0 a_1$$
$$ba_1 = q_1 r_0 a_1 + r_1 a_1$$
$$r_0 a_1 = q_2 r_1 a_1 + r_2 a_1$$
$$\cdots\cdots\cdots$$
$$r_{n-2} a_1 = q_n r_{n-1} a_1 + r_n a_1,$$

dann muß b, da es in aa_1 und ba_1 aufgeht, auch in $ra_1, r_1a_1, r_2a_1, \ldots r_{n-1}a_1$, und schließlich in r_na_1, d. h. in a_1, aufgehen, w. z. b. w.

Aus der Umkehrung dieses Hilfssatzes folgt sofort: wenn zwei Zahlen a sowohl wie a_1 nicht teilbar sind durch eine Primzahl p, so ist auch ihr Produkt aa_1 durch p nicht teilbar, und aus diesem Resultat beweist man endlich noch zum Schluß den folgenden Satz:

Fundamentalsatz. *Eine positive ganze Zahl a läßt sich nur auf eine einzige Weise in ein Produkt aus lauter positiven Primfaktoren zerlegen.*

Beweis. Angenommen für eine ganze Zahl a gelte die Zerlegung

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_\nu$$

und zugleich

$$a = q_1 \cdot q_2 \cdots q_\mu,$$

wo $p_1, p_2, \ldots p_\nu$ und $q_1, q_2 \ldots q_\mu$ zwei Reihen von irgend welchen gleichen oder ungleichen Primzahlen sind. Dann ist a oder das Produkt $p_1 \cdot p_2 \ldots p_\nu$ durch q_μ teilbar, und dies wäre nach dem Hilfssatz nicht möglich, wenn alle Zahlen p von q_μ verschieden wären. Wir dürfen annehmen, daß etwa $p_\nu = q_\mu$ ist und finden ferner durch die gleichen Schlüsse, daß ebenso die Gleichheiten $p_{\nu-1} = q_{\mu-1}$ usw. gelten müssen. Es ist also $\nu = \mu$ zu nehmen und es kann $p_1 = q_1, p_2 = q_2 \ldots$ gesetzt werden.

Übrigens gilt natürlich der Fundamentalsatz allgemein für positive und negative Zahlen und Faktoren, wenn zwei solche Zerlegungen als wesentlich gleich angesehen werden, in welchen sich die Faktoren nur durch das Vorzeichen unterscheiden.

2. Die Funktion $\varphi(m)$.

Aufgabe. Es bedeute m eine beliebige positive ganze Zahl; man soll die Anzahl aller Zahlen aus der Reihe $1, 2, \ldots m$ bestimmen, welche relativ prim zu m sind.

Auflösung. Die gesuchte Anzahl, für ein beliebiges m, bezeichnet man allgemein mit dem Symbol $\varphi(m)$.[1] Wenn m nur eine einzige Primzahl p enthält, so ist offenbar die gesuchte Zahl:

$$\varphi(p) = p - 1 = p\left(1 - \frac{1}{p}\right). \tag{1}$$

1) Dieses Symbol für die von Euler zuerst bestimmte Zahl hat C. F. Gauß eingeführt. Disquisitiones arithmeticae. Sect. II. Art. 38.

Wenn ferner $m = p^k$ ist, so sind in der Reihe $1, 2 \ldots, p^k - 1$ die Zahlen $p, 2p, \ldots (p^{k-1} - 1)p$ die einzigen Zahlen, welche mit p^k einen gemeinsamen Faktor besitzen, daher ist

$$\varphi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k\left(1 - \frac{1}{p}\right). \tag{2}$$

Angenommen nun, es sei m eine beliebige ganze Zahl mit n verschiedenen Primfaktoren, die zu beliebigen Exponenten in m enthalten seien: $m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$; und es werde die gesuchte Anzahl $\varphi(m)$ als bekannt vorausgesetzt, dann soll daraus die Anzahl relativer Primzahlen zu m_1, die kleiner sind als m_1, bestimmt werden, wenn $m_1 = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n} p_{n+1}^{k_{n+1}}$ ist, d. h. einen Primfaktor p_{n+1} zu irgend welchem positiven Exponenten mehr enthält als m. Aus unserer Annahme folgt zunächst, daß es

$$\psi(m_1) = p_{n+1}^{k_{n+1}} \varphi(m) \tag{3}$$

ganze Zahlen gibt, die kleiner sind als m_1, und welche zu $p_1, p_2 \ldots p_n$ prim sind. Denn in jedem Intervall 1 bis $m = \frac{m_1}{p_{n+1}^{k_{n+1}}}$, m bis $2m$, usw. und $(p_{n+1}^{k_{n+1}} - 1)m$ bis $p_{n+1}^{k_{n+1}} m$ gibt es $\varphi(m)$ solcher relativer Primzahlen. Unter diesen $\psi(m_1)$ Zahlen befinden sich aber noch alle Zahlen $< m_1$, welche den Faktor p_{n+1} einfach oder mehrfach enthalten und gleichzeitig zu $p_1 \ldots p_n$ (oder kurz zu m) *prim* sind. Die Anzahl dieser letzteren ergibt sich daraus, daß man in der Reihe

$$1 p_{n+1}, 2p_{n+1}, \ldots \frac{m_1}{p_{n+1}} \cdot p_{n+1}$$

die Zahl derjenigen Faktoren aus $1, 2, \ldots \frac{m_1}{p_{n+1}}$ bestimmt, welche *keine* der Primzahlen $p_1, \ldots p_n$ enthalten oder welche zu m prim sind; dies sind analog der Formel (3):

$$p_{n+1}^{k_{n+1}-1} \varphi(m).$$

Jetzt stellt die Differenz:

$$p_{n+1}^{k_{n+1}} \varphi(m) - p_{n+1}^{k_{n+1}-1} \varphi(m)$$

die Anzahl aller derjenigen Zahlen $< m_1$ dar, welche zu m_1 prim sind, oder welche keine der Primzahlen $p_1, p_2, \ldots p_{n+1}$ als Faktor enthalten, d. h. es ist:

$$\varphi(m_1) = \varphi(m) p_{n+1}^{k_{n+1}} \left(1 - \frac{1}{p_{n+1}}\right). \tag{4}$$

In dieser Gleichung besitzen wir eine Rekursionsformel, aus welcher sich rückwärts die Formel (2) wieder ergibt und aus welcher sich

der explizite Wert von $\varphi(m)$ erschließen läßt, wenn man für m der Reihe nach $1, 2, \ldots, n$ Primfaktoren annimmt.

Sei $m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$, so ist

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right),$$

und das ist die von L. Euler zuerst aufgestellte Formel.

Aus der expliziten Darstellung für $\varphi(m)$ ergeben sich leicht folgende Sätze:

Satz. *Ist $m = m_1 \cdot m_2$ und sind m_1 und m_2 prim zueinander, so ist:*

$$\varphi(m) = \varphi(m_1) \cdot \varphi(m_2).$$

Setzt man noch $\varphi(1) = 1$, so gilt ferner:

Satz. *Ist m eine beliebige ganze Zahl und durchläuft t alle Teiler der Zahl m, dann ist*

$$\sum_t \varphi(t) = m.$$

Beweis. Sei zunächst $m = a = p^k$, dann sind die sämtlichen Teiler von a die Zahlen $1, p, p^2 \ldots p^k$ und folglich ist nach direkter Rechnung:

$$\begin{aligned}\sum \varphi(t_a) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots \varphi(p^k)\\ &= p^k = a.\end{aligned}$$

Im allgemeinen Fall, wenn $m = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n} = a_1 \cdot a_2 \ldots a_n$ gesetzt wird, sieht man leicht, daß alle Teiler von m sich als die einzelnen Glieder des Produktes:

$$(1 + p_1 + \cdots p_1^{k_1})(1 + p_2 + \cdots p_2^{k_2}) \ldots (1 + p_n + \cdots p_n^{k_n})$$

darstellen, indem man dann den direkt vorhergehenden Satz über die Funktion φ zu Hilfe nimmt und auf jeden Teiler anwendet, erhält man eine Summe aus $\varphi(1), \varphi(p_1), \ldots \varphi(p_1)\varphi(p_2), \ldots [\varphi(p_1^{k_1})\varphi(p_2^{k_2}) \ldots \varphi(p_n^{k_n})]$, welche sich wieder als Produkt darstellen läßt in der Form

$$\begin{aligned}\sum \varphi(t) &= \sum \varphi(t_{a_1}) \cdot \sum \varphi(t_{a_2}) \cdots \sum \varphi(t_{a_n})\\ &= a_1 \cdot a_2 \ldots a_n = m.\end{aligned}$$

Der eben bewiesene Satz spielt ein wichtige Rolle in dem Beweise für die Existenz gewisser Zahlen, der gleich nachher einzuführenden Primitivzahlen.

* 3. Kongruenzen.

Wenn ausgedrückt werden soll, daß eine ganze Zahl a durch eine andere ganze Zahl m teilbar ist, daß also $a = m \cdot q$ ist, und

wenn dabei der Quotient $\frac{a}{m} = q$ seinem Wert nach nicht weiter interessiert, so schreibt man nach Gauß[1]) in symbolischer Weise:

$$a \equiv 0 \pmod{m}$$

oder kürzer

$$a \equiv 0, \ (m);$$

gesprochen: a ist kongruent Null modulo m.

Wenn ferner die Differenz zweier ganzer Zahlen a und $b : a - b$ durch m teilbar ist, $a = b + mq$ oder

$$a - b \equiv 0, \ (m)$$

ist, so schreibt man

$$a \equiv b, \ (m);$$

indem man mit der letzteren Schreibweise noch besonders die Tatsache betonen will, daß a und b bei der Division durch m denselben positiven Rest lassen. Die letzte Kongruenz wird gesprochen: a ist kongruent b modulo m (oder nach dem Modul m).

Aus der Definition der Kongruenzen folgt unmittelbar eine Reihe von Tatsachen, deren Beweis so einfach ist, daß wir uns auf die Anführung der Sätze beschränken können:

I. Aus

$$a \equiv b, \ (m)$$

und

$$a \equiv c, \ (m)$$

folgt

$$b \equiv c, \ (m).$$

II. Aus

$$a \equiv b, \ (m)$$

$$c \equiv d, \ (m)$$

folgt

$$a + c \equiv b + d, \ (m).$$

III. Aus

$$a \equiv b, \ (m)$$

$$c \equiv d, \ (m)$$

folgt stets

$$ac \equiv bd, \ (m).$$

Wenn ferner n eine ganze rationale zu m prime Zahl ist, so folgt:

IV. Aus

$$a \equiv b, \ (m)$$

die Kongruenz

$$an \equiv bn, \ (m);$$

---

1) C. F. Gauß, Disquis. arithm. Sect. I. Art. 1, 2.

und insbesondere aus

$$an \equiv bn,\ (m)$$

auch:

$$a \equiv b,\ (m).$$

Diese symbolische Darstellung der Kongruenzen nach Gauß hat sich als eine sehr glückliche und fruchtbringende, überaus bequeme Schreibweise in der Zahlentheorie allgemein eingebürgert.

Es wird durch eine Kongruenz

$$a \equiv b,\ (m)$$

eben sehr anschaulich zum Ausdruck gebracht, daß für zahlentheoretische Überlegungen nur die Tatsache der Teilbarkeit einer Zahl durch eine andere, nicht die Größe des Quotienten von Bedeutung ist. Es ist eine Einteilung aller Zahlen in *Klassen* nach dem Modul m geschaffen, indem zwei Zahlen a und b als nach dem Modul m *gleichwertig, äquivalent,* angesehen werden, wenn sie kongruent sind mod. m, d. h. bei der Division durch m denselben Rest lassen.

Nach einem Modul m verteilen sich die sämtlichen ganzen Zahlen in m Klassen, indem jede Zahl einer und nur einer Zahl der Reihe: $0, 1, 2, \ldots, m-1$ kongruent ist, während keine zwei Zahlen dieser Reihe unter sich kongruent sein können. Die m Zahlen $0, 1, \ldots, m-1$ bilden ein *vollständiges Restsystem* nach dem Modul m, und zwar bezeichnet man dieses als das System der kleinsten Reste. Ein vollständiges Restsystem bilden auch irgend m Zahlen, welche die Eigenschaft haben, daß keine zwei derselben mod. m kongruent sind, eine beliebige ganze Zahl, aber einer und nur einer davon mod. m kongruent ist. Die m ganzen Zahlen zwischen $-\frac{m}{2}$ und $+\frac{m}{2}$ bilden das System der *absolut kleinsten* Reste nach dem Modul m.

4. Der Satz von Fermat.

Satz.[1]) *Wenn p irgend eine rationale Primzahl bedeutet und a nicht teilbar ist durch diese Primzahl, so gilt stets die Kongruenz:*

$$a^{p-1} \equiv 1,\ (p).$$

---

1) Die Bezeichnung „Satz von Fermat“ wird immer für diesen speziellen Satz gebraucht, der von Euler, Lagrange u. a. bewiesen worden ist. Fermat hat die in dem Satze auf S. 11 ausgesprochene allgemeinere Behauptung $a^e \equiv 1, (p)$ ohne Beweis mitgeteilt in einem Brief an Frénicle vom 18. Okt. 1640. Vergl. Oeuvres de Fermat, publ. par P. Tannery et Ch. Henry. tome II. Paris 1894. p. 209.

Beweis. Es sei

$$\left.\begin{array}{r} 1 \cdot a \equiv r_1,\ (p) \\ 2 \cdot a \equiv r_2,\ (p) \\ \cdots\cdots\cdots \\ (p-1) \cdot a \equiv r_{p-1},\ (p) \end{array}\right\} \qquad (1)$$

und es sei ferner festgesetzt, daß die Zahlen $r_1, r_2, \ldots, r_{p-1}$ Zahlen des vollständigen Restsystems $1, 2, \ldots p$ sein sollen, dann stellen die Zahlen $r_1 \ldots r_{p-1}$ die $p-1$ Zahlen $1, 2, 3 \ldots p-1$ in unbekannter Aufeinanderfolge dar. Von den Zahlen r_1 bis r_{p-1} ist nämlich keine gleich 0 oder p und keine zwei derselben können einander mod. p kongruent sein. In der Tat, wenn i und k irgend welche Zahlen der Reihe $1, 2 \ldots p-1$ bedeuten, so kann eine Kongruenz

$$r_i \equiv r_k,\ (p)$$

nur erfüllt sein, wenn i gleich k ist, da sonst $r_i - r_k$ seinem absoluten Betrag nach kleiner ist als p, umsomehr, da $r_i, r_k \leqq p-1$ sind. Dann bleibt nur übrig, daß die Zahlen $r_1, \ldots r_{p-1}$ die Zahlen $1, 2 \ldots p-1$ sind. Das System (1) enthält $p-1$ von einander verschiedene Kongruenzen, durch deren Multiplikation folgt

$$1 \cdot 2 \ldots (p-1) \cdot a^{p-1} \equiv r_1 \cdot r_2 \ldots r_{p-1},\ (p) \qquad (2)$$

oder da

$$r_1 r_2 \ldots r_{p-1} = 1 \cdot 2 \ldots (p-1)$$

ist und das Produkt $1 \cdot 2 \ldots p-1$ zu p prim ausfällt, so bleibt schließlich:

$$a^{p-1} \equiv 1,\ (p). \qquad (3)$$

Für *jede* beliebige ganze Zahl a gilt nun nach dem Modul p die Kongruenz

$$a^p \equiv a,\ (p).$$

Euler hat ferner gezeigt, daß für einen beliebigen ganzzahligen Modul m und für jede zu m prime Zahl a die Kongruenz gilt

$$a^{\varphi(m)} \equiv 1,\ (m).$$

Der Beweis dieses Satzes läßt sich ganz analog dem eben geführten Beweis gestalten.

An den eben behandelten Satz von Fermat schließen sich verschiedene interessante Anwendungen an, von denen wir zunächst die Lösung linearer Kongruenzen anführen wollen.

Aufgabe. Eine Kongruenz

$$ax \equiv b,\ (m)$$

mit bestimmten ganzen Zahlen $a \neq 0$, b, $m \neq 0$ sei gegeben. Man

soll diejenigen ganzen rationalen Zahlen für x angeben, durch welche diese Kongruenz befriedigt ist.

Lösung. 1. Es seien zunächst a und m prim zueinander. Dann ist $a^{\varphi(m)} \equiv 1, (m)$ und aus der Kongruenz $ax \equiv b, (m)$ folgt durch Multiplikation beider Seiten mit $a^{\varphi(m)-1}$:

$$x \equiv b \cdot a^{\varphi(m)-1}, \ (m),$$

so daß also $x = b \cdot a^{\varphi(m)-1}$ eine Lösung der Kongruenz ist. Der Ausdruck

$$b \cdot a^{\varphi(m)-1} + m \cdot s$$

liefert *alle* Lösungen der Kongruenz, wenn s alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchläuft, denn die sämtlichen Lösungen sind einer einzigen mod (m) kongruent. Ist nämlich für zwei verschiedene Werte x_1 und x_2 von x:

$$ax_1 \equiv b, \ (m) \quad \text{und} \quad ax_2 \equiv b, \ (m),$$

so ist

$$a(x_1 - x_2) \equiv 0, \ (m), \quad \text{also} \quad x_1 - x_2 \equiv 0, \ (m),$$

weil ja a prim zu m ist.

2. Zweitens sei $t > 1$ der größte gemeinsame Teiler der Zahlen a und m, dann kann eine ganze rationale Zahl, welche für x gesetzt die Kongruenz $ax \equiv b, (m)$ befriedigt, sicher nur dann gefunden werden, oder kurz, dann ist die Kongruenz nur lösbar, wenn auch b durch t teilbar ist. Dies sieht man leicht ein, wenn man die Kongruenz in der Form

$$\frac{ax - b}{m} = y \quad \text{oder} \quad ax - my = b$$

schreibt, denn in der letzteren Gleichung ist die linke Seite jedenfalls durch t teilbar, folglich muß auch die rechte Seite, d. h. b, durch t teilbar sein. Ist aber diese Bedingung erfüllt und setzt man $a = a_1 t$, $b = b_1 t$, $m = m_1 t$, so sind nun a_1 und m_1 prim zueinander, und es besitzt die gegebene Kongruenz Lösungen, welche offenbar zugleich Lösungen der Kongruenz

$$a_1 x \equiv b_1, \ (m_1)$$

sind und umgekehrt. Schreibt man eine Lösung dieser reduzierten Kongruenz $x_1 = b_1 a_1^{\varphi(m_1)-1}$, so sind alle Lösungen derselben und gleichzeitig der gegebenen Kongruenz in dem Ausdruck

$$b_1 a_1^{\varphi(m_1)-1} + m_1 s = x_1 + m_1 s$$

enthalten, wenn s alle ganzen rationalen Zahlen durchläuft.

Unter diesen Zahlen sind aber die Werte

$$x_1, \ x_1 + m_1, \ x_1 + 2m_1, \ \ldots \ x_1 + (t-1)m_1$$

modulo m inkongruent, und so viele, nämlich t modulo m inkongruente Lösungen besitzt also die gegebene Kongruenz.

Die Resultate unter 1. und 2. können wir auch in folgender modifizierter Weise zusammenfassen:

Satz. *Die Diophantische Gleichung*

$$ax - my = b$$

mit den ganzen rationalen Zahlenkoeffizienten a, b, m besitzt dann und nur dann unendliche viele Lösungen, wenn der größte gemeinsame Teiler t der Zahlen a und m auch in b aufgeht.

Die Lösungen, d. h. die Zahlenwerte für x bezw. y, sind durch t nach dem Modul m bez. a inkongruente Zahlen darstellbar.

Nach diesem Satze kann man insbesondere zu zwei gegebenen ganzen Zahlen a, b mit dem größten gemeinsamen Teiler t stets zwei ganze Zahlen x, y so finden, daß $ax + by = t$ wird.

Unter Benützung dieses Satzes ergibt sich hier noch eine zweite Anwendung des Fermatschen Satzes:

Satz. *Bedeutet p eine positive rationale Primzahl und a eine durch p nicht teilbare ganze Zahl, so ist der kleinste positive Exponent e, für welchen die Kongruenz*

$$a^e \equiv 1, (p)$$

erfüllt ist, ein Teiler der Zahl $p - 1$.

Da a prim ist zu p, muß, abgesehen von dem Fall $a = 1$ resp. $a \equiv 1, (p)$, der Exponent $e > 1$ sein. Zunächst überzeugt man sich, daß alle Potenzen $a^1, a^2, \ldots a^{e-1}$ mod (p) verschieden sind, denn aus

$$a^{e_1} \equiv a^{e_2}, (p) \quad \text{folgt} \quad a^{p-1-e_2} a^{e_1} \equiv a^{p-1}, (p),$$

d. h. $a^{e_1 - e_2} \equiv 1, (p)$, und dies ist nach Voraussetzung nur möglich, wenn $e_1 - e_2 = e$ ist, also nicht dann, wenn e_1 und $e_2 \leqq e$. Angenommen e wäre *kein* Teiler von $p - 1$, so kann man zwei ganze rationale Zahlen x, y angeben, daß $ex + (p-1)y = e'$ wird, wo e' der größte gemeinsame Teiler von e und $p - 1$ ist. Aus $a^e \equiv 1$, $a^{p-1} \equiv 1, (p)$ folgt aber dann auch $a^{ex} a^{(p-1)y} \equiv 1$, oder $a^{e'} \equiv 1, (p)$. Da dabei $e' < e$ sein müßte, so widerspricht dies der vorausgehenden Bemerkung. e ist daher selbst ein Teiler von $p - 1$.

Die Beziehung der Zahlen a und e drückt man so aus, daß man sagt, a gehöre zum Exponenten e.

Von besonderer Bedeutung sind nun diejenigen ganzen Zahlen w, welche zum Exponenten $p - 1$ selbst gehören. Die aufeinander folgenden Potenzen einer solchen

$$w, w^2, w^3, \ldots w^{p-1}$$

stellen mod. m die zu p primen Zahlen $1, 2, \ldots p-1$ des vollständigen Restsystems, in unbekannter Anordnung allerdings, dar. Nach Euler heißen diese Zahlen w *Primitivzahlen nach* p, und Gauß[1]) hat nach einem berühmten Schlußverfahren, das wir jedoch erst für die quadratischen Zahlen anführen wollen, folgenden Existenzsatz bewiesen:

Satz. *Zu jedem Teiler* e *der Zahlen* $p-1$ *gehören* $\varphi(e)$ *nach dem Modul* p *inkongruente Zahlen, insbesondere gibt es stets* $\varphi(p-1)$ *nach dem Modul* p *verschiedene Primitivzahlen nach* p.

Beispiel. Es sei z. B. $p = 7$, so gehören zum Teiler e von $p - 1 = 6$

$1 : \varphi(1) = 1$ Zahlen, nämlich $a = 1$,
$2 : \varphi(2) = 1$ „ „ $a = 6$,
$3 : \varphi(3) = 2$ „ „ $a = 2, 4$,
$6 : \varphi(6) = 2$ „ „ $a = 3, 5$.

Bei dem Beweis dieses Satzes wird man u. a. auch auf Kongruenzen geführt, welche eine unbekannte Größe x enthalten, von der Form

$$a_0 x^n + a_1 x^{n-1} + \cdots a_n \equiv 0, \ (a)$$

mit ganzen rationalen Koeffizienten a.

Wenn $a_0 \not\equiv 0, (a)$ ist, so heißt eine solche Kongruenz ganz und rational vom Grad n. Für diese Kongruenzen gelten ähnliche Sätze wie für Gleichungen.

Bezeichnet man eine ganze rationale Zahl x_1, welche statt x in den Ausdruck auf der linken Seite eingesetzt die Kongruenz befriedigt, als *Wurzel* der Kongruenz, dann gilt der folgende Satz.

Satz. Wenn die Kongruenz $f(x) = a_0 x^n + \cdots a_n \equiv 0, (p)$ nach dem Primzahlmodul p eine Wurzel besitzt, so gibt es stets eine Wurzel x_1, so daß $f(x_1) \equiv 0, (p)$, nicht aber $f(x_1) \equiv 0, (p^2)$ ausfällt.

Ist nämlich für $x = a : f(a) \equiv 0, (p^2)$, so kann man l als ganze Zahl so bestimmen, daß $x_1 = a + lp$ dem Satz genügt.

Ganz ähnlich wie man in der Algebra den Satz beweist, daß eine Gleichung n^{ten} Grades $f(x) = 0$ höchstens n Wurzeln besitzt, zeigt man die Richtigkeit des folgenden Satzes:

Satz. *Eine Kongruenz* n^{ten} *Grades nach einem Primzahlmodul* p

$$a_0 x^n + a_1 x^{n-1} + \cdots a_n \equiv 0, \ (p)$$

besitzt höchstens n *nach dem Modul* p *verschiedene Wurzeln.*

---

1) Disqu. arithm. III, 52 bis 55.

Es braucht aber allerdings die Kongruenz nicht gerade n Wurzeln zu besitzen, vielmehr kann die Anzahl der Wurzeln kleiner als n, ja sogar Null sein. Die Entscheidung, ob eine Kongruenz Lösungen besitzt, ist für jede Kongruenz besonders zu treffen. Am einfachsten ist dies natürlich für $n = 2$.

Eine Kongruenz zweiten Grades nach einem Primzahlmodul p kann stets auf die Form gebracht werden:

$$x^2 - m \equiv 0, \ (p).$$

Falls diese Kongruenz eine Wurzel w besitzt, so besitzt sie auch die Wurzel $-w$. Wenn dann m prim ist zu p, so sagt man, m sei *quadratischer Rest* nach p, falls aber die Kongruenz unlösbar ist, heißt m *quadratischer Nichtrest* nach p. Legendre[1]) hat zur Bezeichnung dieser Möglichkeiten ein allgemein eingebürgertes Symbol gebraucht, er setzt für ein m, das nicht teilbar ist durch p, und für $p > 2$:

$$\left(\frac{m}{p}\right) = +1, \text{ wenn } m \text{ quadratischer Rest nach } p \text{ ist,}$$

$$\left(\frac{m}{p}\right) = -1, \text{ wenn } m \text{ quadratischer Nichtrest nach } p \text{ ist.}$$

Unter der vorigen Voraussetzung über m und p hat also das Symbol $\left(\frac{m}{p}\right)$ stets einen der beiden Werte ± 1, und es heißt $+1$, resp. -1, der Restcharakter der Zahl m nach p. Die Berechnung dieses Wertes ergibt sich später, Nr. 25. Doch können schon hier auf Grund des Satzes von der Existenz der Primitivzahlen einige Rechnungsregeln für das Symbol entwickelt werden.

Bezeichnet w eine Primitivzahl nach der ungeraden Primzahl p, dann gibt es einen ganz bestimmten Exponenten M, für welchen

$$m \equiv w^M, \ (p)$$

ist. Die Kongruenz

$$x^2 - w^M \equiv 0, \ (p)$$

ist jetzt offenbar dann und nur dann lösbar, wenn M eine *gerade* Zahl bezeichnet.

Hieraus folgt unmittelbar ein von Euler aufgestellter Satz in der folgenden Formulierung:

Satz. *Die Zahl m ist quadratischer Rest oder Nichtrest nach der ungeraden Primzahl p, je nachdem*

---

1) Legendre, Zahlentheorie, übers. v. Maser, Bd. I, p. 198.

$$m^{\frac{p-1}{2}} \equiv +1, (p) \quad \text{oder} \quad m^{\frac{p-1}{2}} \equiv -1, (p)$$

sich ergibt, oder es ist stets:

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}}, (p).$$

Sind m, m_1 irgend zwei beliebige ganze Zahlen, von welchen bloß keine durch p teilbar sein soll, und setzt man

$$m \equiv w^M, (p), \quad \text{ferner} \quad m_1 \equiv w^{M_1}, (p),$$

so ist

$$m m_1 \equiv w^{M+M_1}, (p),$$

$$\left(\frac{m \cdot m_1}{p}\right) \equiv (m m_1)^{\frac{p-1}{2}}, (p),$$

oder

$$\left(\frac{m}{p}\right)\left(\frac{m_1}{p}\right) = \left(\frac{m \cdot m_1}{p}\right),$$

und diese Zerlegung ist schon ein erster Schritt zur Berechnung des allgemeinen Legendreschen Symbols. Es stellt die letzte Gleichung die Multiplikationsregel für das Symbol vor, durch welche die Berechnung desselben zurückgeführt wird auf den Fall $\left(\frac{q}{p}\right)$, wo q und p Primzahlen bedeuten. Speziell für negative m ergibt sich

$$\left(\frac{-m}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{+m}{p}\right).$$

Hiermit kann die Aufzählung von Tatsachen aus der elementaren Theorie der rationalen Zahlen abgebrochen werden. Ich wende mich gleich zur Untersuchung allgemeiner algebraischer Zahlen, um dann erst im Anschluß hieran wieder auf die eben angeschnittenen Fragen zurückzukommen.

Die Theorie der algebraischen Zahlen ist ein noch verhältnismäßig junger Zweig der Zahlentheorie, dessen Entwicklung von Gauß angeregt und eingeleitet worden ist. Euler, dann Legendre und Gauß hatten unabhängig voneinander die Entdeckung gemacht, daß für die Lösungen von zwei quadratischen Kongruenzen mit ungeraden Primzahlen p und q: $x^2 - q \equiv 0, (p)$ und $x^2 - p \equiv 0, (q)$ eine sehr

merkwürdige Reziprozität stattfindet, welche sich in der Gleichung $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ aussprechen läßt. Es war Gauß zuerst gelungen, dieses Reziprozitätsgesetz einwandfrei zu beweisen, indem er sechs auf ganz verschiedenen Prinzipien beruhende Beweise entwickelte. Als nun Gauß[1]) daran ging, dieses Fundamentaltheorem auf höhere Kongruenzen zu übertragen, und dabei speziell die Kongruenzen vierten Grades $x^4 - q \equiv 0,\ (p)$ betrachtete, fand er wohl eine große Reihe spezieller Sätze, das allgemeine „biquadratische" Reziprozitätsgesetz blieb aber bei der Beschränkung auf rationale reelle Zahlen verschleiert, und die Beweise, die für die speziellen Sätze ausgereicht hatten, ließen sich durchaus nicht auf allgemeine rationale Zahlen erweitern. Die Schwierigkeiten[2]) schwanden, es fand sich ein allgemeines und durchsichtiges Reziprozitätsgesetz, nachdem Gauß zu einer „eigentümlichen Erweiterung des ganzen Feldes der höheren Arithmetik" geschritten war und den komplexen Zahlen $a + b\sqrt{-1}$ das „völlig gleiche Bürgerrecht" mit den reellen ganzen Zahlen einräumte.[3])

Diese Tat hat seitdem reiche Früchte getragen. Gauß hat hier mit dem glücklichen Instinkte des Genies der Wissenschaft neue und überreiche Gebiete eröffnet. Bald[4]) zeigte sich, daß das kubische Reziprozitätsgesetz am einfachsten sich darstellen läßt, wenn man die Zahlen $a + b\,\frac{1+\sqrt{-3}}{2}$ zu Grunde legte, und Analoges[4]) ergab sich für die höheren Reziprozitätsgesetze. Die Frage nach der Lösbarkeit der unbestimmten Gleichung $x^n + y^n = z^n$ erforderte ganz von selbst die Berücksichtigung komplexer Zahlen, welche aus n^{ten} Einheitswurzeln gebildet sind, und auch auf dem Gebiete der elliptischen Funktionen für die Theorie der komplexen Multiplikation erwies sich die Heranziehung von Zahlen $a + b\sqrt{m}$ als notwendig.

Der hauptsächlichste Wert, welchen die Ausbildung der Lehre von den Zahlkörpern für die Zahlentheorie besitzt, ist indessen darin zu suchen, daß sie diese um viele *allgemeine Methoden* bereichert hat, wie man wohl aus den folgenden Behandlungen einzelner Kapitel der Körpertheorie ersehen wird. Mehr und mehr verträgt heute die

---

1) C. F. Gauß, Theoria residuorum biquadraticorum. Ges. Werke, Bd. II, p. 67 und Besprech. p. 165.

2) C. F. Gauß, Werke, Bd. II, p. 95 und p. 169.

3) C. F. Gauß, Werke, Bd. II, p. 171. Anzeige aus dem Jahre 1831.

4) C. G. F. Jacobi, Ges. Werke, Bd. VI, p. 233, 275 und G. Eisenstein, Beweis des Reziprozitätsges. für kub. Reste. Crelles Journal Bd. 27 und 28.

Zahlentheorie nach den von Gauß so glänzend eingeleiteten Entdeckungen der Zahlentheoretiker des letzten Jahrhunderts mit Bezug auf ihre reichen und weitreichenden *Methoden* einen Vergleich mit der allgemeinen Analysis, so daß sie auch nicht mehr bloß, wie einst, das Besitztum weniger bevorzugter Geister ist.

Die Arithmetik der komplexen Zahlen

$$a + b\sqrt{-1} \quad \text{oder} \quad a + b\,\frac{1+\sqrt{-3}}{2}$$

erfordert keine wesentlich neuen Prinzipien gegenüber der elementaren reellen Zahlentheorie. Sie läßt sich als eine Verallgemeinerung dieser letzteren unschwer entwickeln und ist mehrfach dargestellt[1]) worden. Um nicht durch Wiederholungen zu ermüden, sollen hier, zur Einführung, die Hauptresultate angeführt werden, zu denen die Beweise ja alle im folgenden enthalten sind.

Eine komplexe Zahl $a + b\sqrt{-1}$ ist „ganz", wenn a, b ganze rationale Zahlen sind. Die Summe, Differenz und das Produkt von irgend zwei ganzen komplexen Zahlen, ist wieder eine ganze komplexe Zahl. Sind ferner α, β, γ drei ganze komplexe Zahlen und $\alpha = \beta \cdot \gamma$, so sagt man α ist teilbar durch β oder γ; oder auch β geht in α auf. Es gibt außer ± 1 noch die zwei ganzen Zahlen $\pm\sqrt{-1}$, welche in 1 aufgehen, und die vier Zahlen ± 1, $\pm\sqrt{-1}$ heißen die Einheiten des Körpers.

Da man nun zeigen kann, s. S. 29, daß für irgend zwei ganze Zahlen α und β ein Euklidisches Teilerverfahren gilt, so läßt sich der Begriff der Primzahl erweitern, und es gilt der Satz: Jede ganze komplexe Zahl läßt sich im wesentlichen nur auf eine Weise in Primfaktoren zerlegen, wenn man von Einheitsfaktoren absieht.

Jede komplexe Primzahl ist Faktor einer reellen Primzahl, und zwar zerfällt: die Zahl 2 in $(1+\sqrt{-1})(1-\sqrt{-1})$, ferner jede Primzahl $p \equiv 1$, (4) in zwei voneinander verschiedene Primzahlen $\pi = x + y\sqrt{-1}$ und $\pi' = x - y\sqrt{-1}$; dagegen ist jede reelle Primzahl $p \equiv 3$, (4) auch Primzahl im Gebiete der komplexen Größen.

Jede komplexe ganze Zahl $a + b\sqrt{-1}$ kann als Modul von linearen, quadratischen und anderen Kongruenzen angesetzt werden, die Lehre dieser letzteren überträgt sich in einfacher Weise auf die komplexen Zahlen. Zu jeder Zahl $a + b\sqrt{-1} = \alpha$ gibt es ein System

---

1) C. F. Gauß, l. c.; Dirichlet-Dedekind, Vorlesungen, Suppl. XI, p. 435.

von $a^2 + b^2$ Zahlen, so daß keine zwei derselben einander nach dem Modul α kongruent sind, während aber *jede* beliebige reelle oder komplexe Zahl *einer* der Zahlen des Systems kongruent ist.

Der Fermatsche Satz lautet für die komplexen Zahlen:

Ist $\pi = x + y\sqrt{-1}$ eine komplexe Primzahl und α irgend eine durch dieselbe nicht teilbare ganze Zahl, so ist stets:

$$\alpha^{x^2+y^2-1} \equiv 1, \ (\pi);$$

und es lassen sich hieran der Begriff der Primitivwurzeln und die Untersuchung quadratischer Kongruenzen sowie des Reziprozitätsgesetzes anschließen.

Zweiter Abschnitt.

Der quadratische Zahlkörper.

5. Einleitung und Definitionen.

Der Name *Zahlkörper*, auch *Zahlbereich* oder *Bereich* ist der Nomenklatur der allgemeinen Zahlentheorie, oder Algebra, entnommen und ist von Dedekind bezw. von Kronecker in die Wissenschaft eingeführt. Er bezeichnet ein unendliches System von Größen, in welchem die Grundoperationen der Addition, Subtraktion, Multiplikation und Division unbeschränkt ausführbar sind, indem das Resultat jener Operationen mit irgend welchen Größen des Systems, abgesehen von der Division einer Größe durch 0, immer wieder eine Größe des Systems ist.

Man pflegt z. B. zu sagen, daß die sämtlichen rationalen Zahlen einen Körper bilden oder einem Bereich angehören. Bedeuten a, b, x, ... irgendwelche rationale Zahlen, so ist in der Ausdrucksweise der Algebra jede lineare Gleichung $ax + b = 0$, oder $a + x = b$ im Bereich oder Körper der rationalen Zahlen unbeschränkt lösbar, falls nicht im ersten Beispiel $a = 0$ ist.

Dagegen ist nicht jede quadratische Gleichung $ax^2 + b = 0$ oder $ax^2 + bx + c = 0$, deren Koeffizienten dem Bereich der rationalen Zahlen angehören, in diesem Bereich auch lösbar. Diese Gleichungen *werden* erst lösbar, wenn man dem Körper der rationalen Zahlen Ausdrücke von der Form $\sqrt{m}$ „adjungiert", wo m eine ganze rationale Zahl bezeichnen kann.

Man *erweitert* damit den Begriff der Zahl, indem man auch alle Ausdrücke von der Gestalt $u + v\sqrt{m}$ *Zahlen* nennt, wenn u, v rationale Zahlen bedeuten. Zur Unterscheidung von den natürlichen Zahlen heißen die Zahlen $u + v\sqrt{m}$ **algebraische Zahlen.** Jede solche Zahl genügt offenbar einer quadratischen Gleichung $ax^2 + bx + c = 0$ mit ganzen rationalen Koeffizienten, und man bezeichnet darum die Ausdrücke $u + v\sqrt{m}$ auch speziell als **quadratische Zahlen.**

Es sei m eine ganze rationale, im übrigen aber beliebige Zahl, und $\sqrt{m}$ die mit dem positiven Vorzeichen versehene Wurzel der Gleichung $x^2 - m = 0$, so adjungieren wir dem Bereich der rationalen

Zahlen diese Größe $\sqrt{m}$ und nehmen in dem so erweiterten Zahlenbereich die vier elementaren Operationen, der Addition, Subtraktion, Multiplikation und Division, in unbeschränkter Folge vor, dann erhalten wir die sämtlichen rationalen Funktionen der Größe $\sqrt{m}$. Weil aber $(\sqrt{m})^2 = m$, $(\sqrt{m})^3 = m\sqrt{m}$ usw. usw. ist, so sind die sich ergebenden Ausdrücke alle von der Form:

$$\frac{a + b\sqrt{m}}{a_1 + b_1\sqrt{m}},$$

oder noch einfacher:

$$\frac{a + b\sqrt{m}}{c},$$

worin a, b, c, a_1, b_1 jetzt wieder ganze rationale Zahlen, oder die Zahl Null bedeuten, indem nur der Fall, daß a_1 und b_1 resp. c allein Null sind, ausgeschlossen bleibt.

Die rationalen Funktionen von $\sqrt{m}$ bilden in dem oben definierten Sinne einen **Rationalitätsbereich**[1]) oder einen **Zahlkörper**[2]), auch kurzweg **Körper** (nach Dedekind), da die Summe, Differenz, das Produkt oder der Quotient zweier solcher Funktionen wieder von derselben Form ist. Wir benützen die zweite Bezeichnung und benennen insbesondere den soeben definierten speziellen Körper als einen *quadratischen Zahlkörper*. Derselbe ist durch die Zahl $\sqrt{m}$ vollständig bestimmt, weshalb er bequem mit $k(\sqrt{m})$ geschrieben wird.

Wo keine Zweideutigkeit zu befürchten ist, kann auch kurz der „*Körper k*" geschrieben werden.

Es ist klar, daß auch der Körper der rationalen Zahlen ein ganz spezieller quadratischer Zahlkörper ist, und daß jeder quadratische Zahlkörper $k(\sqrt{m})$ den Körper der rationalen Zahlen vollständig enthält. Ganz allgemein ist die Ausdrucksweise gebräuchlich: Der Zahlkörper $k(\sqrt{m})$ entsteht aus dem Körper der rationalen Zahlen, indem man dem letzteren die Größe $\sqrt{m}$ adjungiert.

Unmittelbar einleuchtend sind jetzt folgende Behauptungen:

1. Der Zahlkörper $k(-\sqrt{m})$ ist identisch mit dem Zahlkörper $k(\sqrt{m})$.

---

1) L. Kronecker, Grundzüge einer arithmet. Theorie der algebr. Größen, 1882, Werke, Bd. II, S. 248.

2) Dirichlet-Dedekind, Vorlesungen, 4. Aufl., Suppl. XI, p. 452. In diesem Suppl. findet man die in dieser und den folgenden Nummern erwähnten Begriffe eingeführt. Für die Beweise vergl. bes. Hilbert, Zahlb. Kap. I bis III und XVI.

2. Ist δ eine Wurzel der Gleichung:

$$a_0 x^2 + 2a_1 x + a_2 = 0 \quad \text{und} \quad m = a_1^2 - a_0 a_2,$$

so ist der Körper $k(\delta)$ identisch mit dem Zahlkörper $k(\sqrt{m})$ und zwar definieren beide Wurzeln δ_1, δ_2 der Gleichung zweiten Grades denselben Zahlkörper.

Nach dieser Ausdehnung des Zahlbegriffs erhebt sich nun als erste Frage: Was entspricht dem Begriff der ganzen rationalen Zahl und der gebrochenen rationalen Zahl im quadratischen Zahlkörper?

Die Ausdehnung des Begriffs „ganz" auf den allgemeineren Zahlenbereich wird man zweckmäßig so vornehmen, daß der erweiterte Begriff im spezielleren, nämlich rationalen, Zahlkörper seine Geltung behält, d. h. daß eine ganze Zahl des quadratischen Zahlkörpers, welche rational ist, zugleich eine rationale ganze Zahl ist. Man wird ferner vor allem die Forderung stellen, daß im quadratischen wie im rationalen Zahlkörper der Begriff „ganz" für dieselben Rechenoperationen invariant bleibt, d. h. daß bei denselben Rechenoperationen ganze Zahlen immer wieder nur ganzzahlige Resultate liefern. Es ist für die ganzen rationalen Zahlen charakteristisch, daß die *Summe*, die *Differenz* und das *Produkt* zweier ganzer Zahlen jedesmal wieder eine ganze rationale Zahl ist, und man verlangt, daß diese Eigenschaften der ganzen Zahlen auch im quadratischen Zahlkörper noch gelten. Schließlich soll jede Zahl eindeutig, in der einfachsten Form auftreten, d. h. wenn eine ganze Zahl in der Gestalt

$$\frac{a + b\sqrt{m}}{c}$$

angenommen wird, sollen Zähler und Nenner dieses Bruches nicht einen überflüssigen gemeinsamen Teiler haben.

Diesen Anforderungen genügt folgende Definition:

Definition. *Eine Zahl eines quadratischen Zahlkörpers heißt eine ganze quadratische Zahl, wenn sie einer Gleichung zweiten Grades genügt:*

$$x^2 + a_1 x + a_2 = 0,$$

in welcher der Koeffizient des höchsten Gliedes gleich 1 *ist, während die Koeffizienten a_1 und a_2 ganze rationale Zahlen sind.*

Aus dieser Definition folgt sofort folgender Satz:

Satz. *Jede ganze Zahl eines quadratischen Zahlkörpers, welche rational ist, ist zugleich eine ganze rationale Zahl.*

Beweis. Es sei α eine ganze Zahl des Körpers und genüge der Gleichung:

$$x^2 + a_1 x + a_2 = 0.$$

Ist nun die Zahl α rational, so kann sie als Quotient zweier *ganzer* rationaler Zahlen a und b in der Form $\alpha = \frac{a}{b}$ dargestellt werden, wobei man voraussetzen darf, daß a und b teilerfremd sind. Dann wäre also:

$$\frac{a^2}{b^2} + a_1 \frac{a}{b} + a_2 = 0,$$

oder

$$\frac{a^2}{b} = -(a_1 a + a_2 b).$$

Da rechts eine ganze rationale Zahl steht, so muß auch $\frac{a^2}{b}$ ganz sein, was verlangt, daß $b = 1$ ist, weil a und b außer 1 keinen Teiler gemein haben, es bleibt also nur übrig, daß $\alpha = a$ selbst eine ganze rationale Zahl ist.

Bezeichnung. Wir wollen künftig durchgängig die (ganzen) quadratischen Zahlen mit kleinen griechischen Buchstaben α, β, γ, $\delta \ldots \omega \ldots$ bezeichnen und die absoluten Beträge, wie üblich, mit $|\alpha|$ usw.

6. Der Zahlkörper $k(\sqrt{m})$.
Die ganzen Zahlen und die Basis des Körpers.

Es erleichtert die Darstellung und die Untersuchung der neuen Begriffe wesentlich, wenn über die den Körper bestimmende Zahl $\sqrt{m}$ die Voraussetzung gemacht wird, daß m *eine ganze rationale Zahl ohne quadratische Faktoren* sein soll.

Wir werden diese Voraussetzung dauernd festhalten und können dies umso eher tun, als sich zeigen läßt, daß die Betrachtung der Körper $k(\sqrt{m})$ für ganz beliebige m auf den speziellen Fall zurückführt.

Alle Zahlen des Körpers $k(\sqrt{m})$ sind von der Gestalt:

$$\frac{a + b\sqrt{m}}{c}.$$

Ist m eine positive Zahl, so enthält der Körper $k(\sqrt{m})$ *nur reelle* Zahlen und heißt danach ein *reeller Körper*. Ist aber m eine negative Zahl, so sind alle Zahlen $u + v\sqrt{m}$, falls $v \neq 0$, imaginär resp. komplex und $k(\sqrt{m})$ heißt dann ein *imaginärer Körper*.

Zu jeder Zahl $\alpha = \frac{a + b\sqrt{m}}{c}$ gehört eine *konjugierte* Zahl $\alpha' = \frac{a - b\sqrt{m}}{c}$, welche dadurch charakterisiert ist, daß α und α' der-

selben quadratischen Gleichung mit rationalen Koeffizienten genügen, und welche aus α hervorgeht, wenn man darin die Größe $+\sqrt{m}$ durch $-\sqrt{m}$ ersetzt. Die zu α konjugierte Zahl soll stets durch denselben Buchstaben mit dem Akzent, also mit α', bezeichnet werden.

Wenn α eine ganze Zahl des Körpers ist, so ist auch α' ganz und umgekehrt. Es ist ohne weiteres nach der Definition der ganzen Zahlen klar, daß jede Zahl $a + b\sqrt{m}$ ganz ist, falls a, b ganze rationale Zahlen sind. Ganz allgemein läßt sich jede ganze Zahl in der Gestalt $\frac{a + b\sqrt{m}}{c}$ annehmen, wobei a, b, c drei ganze rationale Zahlen *ohne gemeinsamen Teiler* sind, und wir wollen aus jener Definition noch einige weitere Folgerungen ziehen über die Form der ganzen Zahlen, indem wir untersuchen, ob der Nenner c in dem Ausdruck $\frac{a + b\sqrt{m}}{c}$ auch andere Werte als $c = 1$ annehmen kann. Die Zahl α befriedigt die Gleichung:

$$x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 m}{c^2} = 0,$$

und ist nach Definition nur dann eine ganze Zahl, wenn

$$\frac{2a}{c} \quad \text{und} \quad \frac{a^2 - b^2 m}{c^2}$$

ganze rationale Zahlen sind.

Angenommen c enthalte eine Primzahl $p > 2$ als Faktor. Dann muß auch a den Faktor p enthalten, damit $\frac{2a}{c}$ ganz ist. Ferner muß dann p^2 in $a^2 - b^2 m$ aufgehen, und weil a^2 durch p^2 teilbar ist, muß $b^2 m$ durch p^2 teilbar sein. Die Zahl m enthält aber nach Voraussetzung keinen quadratischen Faktor, es bleibt also mindestens die Bedingung $b^2 \equiv 0, (p)$ übrig, die sicher nur erfüllt ist, falls auch b selbst durch p teilbar ist. Diese Folgerung widerspricht indessen der Annahme über a, b, c. Es kann bei beliebigen a, b, c der Nenner c außer etwa der Zahl 2 nur solche Faktoren enthalten, welche in a und b gleichzeitig aufgehen. Man zeigt weiter auf die nämliche Weise, daß c allein auch nicht eine höhere Potenz als 2 enthalten kann, und daher sind alle ganzen Zahlen schon in der Form $\frac{a + b\sqrt{m}}{2}$ enthalten. Es ist unmittelbar einzusehen, daß für $a = 0$ und $b \neq 0$, oder aber für $b = 0$ und $a \neq 0$ die nichtverschwindenden Zahlen b bezw. a durch c teilbar sein müssen, oder daß $c = 1$ sein muß. Die Untersuchung der übrigen Möglichkeiten führt auf folgenden Satz:

Satz. *Jede ganze Zahl des quadratischen Zahlkörpers* $k(\sqrt{m})$ *läßt sich darstellen:*

1. *durch die Formel*

$$a + b\,\frac{1+\sqrt{m}}{2},$$

im Falle, daß $m \equiv 1,\ (4)$ *ist,*

2. *durch die Formel*

$$a + b\sqrt{m},$$

im Falle, daß $m \equiv 2,\ (4)$, *oder* $m \equiv 3,\ (4)$ *ist, wobei* a, b *irgendwelche ganze rationale Zahlen bedeuten.*

Beweis. 1. Fall, $m \equiv 1,\ (4)$. Wenn a, b beliebige ganze rationale Zahlen bezeichnen, so ist die Zahl $\alpha = \frac{a+b\sqrt{m}}{2}$ ganz, wenn $\frac{2a}{2}$ und $\frac{a^2-b^2m}{4}$ ganz sind. Die erste Bedingung ist offenbar stets erfüllt, dagegen ist $a^2 - b^2m \equiv 0,\ (4)$ nur dann erfüllt, wenn entweder a und b gleichzeitig *gerade*, oder wenn a und b zugleich *ungerade* sind. Entsprechend diesen beiden Möglichkeiten ergibt sich für eine ganze Zahl α entweder die Form:

$$\alpha = \frac{2a_1 + 2b_1\sqrt{m}}{2} = a_1 + b_1\sqrt{m},$$

oder:

$$\alpha = \frac{(2a_1+1)+(2b_1+1)\sqrt{m}}{2} = a_2 + b_2\,\frac{1+\sqrt{m}}{2}.$$

Beide Formen sind aber in dem Ausdruck $a + b\,\frac{1+\sqrt{m}}{2}$ enthalten, und man sieht auch unmittelbar sofort ein, daß dieser Ausdruck bloß ganze Zahlen darstellt.

2. Fall, $m \equiv 2,\ (4)$ oder $m \equiv 3,\ (4)$. In diesem Fall ist die Zahl $\alpha = \frac{a+b\sqrt{m}}{2}$ ganz, wenn $a^2 - b^2m \equiv 0,\ (4)$ ausfällt. Weil aber das Quadrat einer ganzen Zahl entweder $\equiv 0$, oder $\equiv 1,\ (4)$ ausfällt, so müssen a und b beide gerade sein. Alle ganzen Zahlen des Körpers sind somit von der Gestalt $a + b\sqrt{m}$.

Setzen wir von jetzt ab:

$$1.\quad \omega = \frac{1+\sqrt{m}}{2}, \quad \text{falls} \quad m \equiv 1,\ (4),$$

$$2.\quad \omega = \sqrt{m} \qquad \text{falls} \quad m \not\equiv 1,\ (4),$$

so ist also jede ganze Zahl eines Körpers $k(\sqrt{m})$ durch einen linearen Ausdruck

$$a \cdot 1 + b\omega$$

mit irgendwelchen rationalen ganzen Zahlen a, b darstellbar.

Man nennt die Zahlen

$$1 \text{ und } \omega$$

eine **Basis** des Zahlkörpers, indem für dieselbe allgemein folgende Definition gilt:

Definition. *Unter einer Basis eines quadratischen Zahlkörpers versteht man zwei ganze Zahlen ω_1, ω_2 des Körpers von der Beschaffenheit, daß jede andere ganze Zahl des Körpers durch einen linearen Ausdruck:*

$$a\omega_1 + b\omega_2,$$

mit bestimmten ganzen rationalen Koeffizienten a und b auf eine einzige Weise darstellbar ist.

Es gibt unendlich viele Zahlenpaare ω_1, ω_2, welche als Basis des Körpers $k(\sqrt{m})$ genommen werden können.

In der Tat, wenn ω_1 und ω_2 zwei ganze Zahlen sind, so bestehen ja die Beziehungen:

$$\omega_1 = a_1 + b_1\omega$$
$$\omega_2 = a_2 + b_2\omega,$$

und es bilden ω_1 und ω_2 eine Basis des Körpers dann, wenn die Gleichung gilt:

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \pm 1.$$

Unter dieser Bedingung ist nämlich:

$$1 = \frac{b_2\omega_1 - b_1\omega_2}{\pm 1}$$
$$\omega = \frac{-a_2\omega_1 + a_1\omega_2}{\pm 1},$$

daher gilt für irgendeine Zahl α^* eine Darstellung:

$$\alpha^* = a^*\omega_1 + b^*\omega_2.$$

Andererseits erhält man auch *jede* ganze Zahl α des Körpers, wenn a^*, b^* *alle* rationalen ganzen Zahlen durchlaufen.

Die Gleichung

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = a_1b_2 - a_2b_1 = \pm 1$$

kann für unendlich viele ganzzahlige Wertsysteme a_1, b_1, a_2, b_2 befriedigt werden, denn man darf für a_1, b_1 irgendwelche teilerfremde Zahlen wählen und kann dann stets a_2, b_2 der letzten Gleichung entsprechend bestimmen. Es gibt also unendlich viele Paare von Basiszahlen.

Satz. *Bilden ω_1, ω_2 und ω_1^*, ω_2^* zwei verschiedene Systeme von Basiszahlen eines Körpers, und gilt die Darstellung*

$$\omega_1^* = a_1\omega_1 + b_1\omega_2$$
$$\omega_2^* = a_2\omega_1 + b_2\omega_2,$$

so ist stets

$$a_1 b_2 - a_2 b_1 = \pm 1.$$

Der Beweis ergibt sich unmittelbar aus der Darstellung von ω_1, ω_2 durch die Basis ω_1^*, ω_2^*.

Auf Grund der bisherigen Resultate läßt sich nun weiter die folgende Behauptung beweisen:

Satz. *Die Summe, Differenz, sowie das Produkt irgend zweier ganzer Zahlen α, β des Körpers ist wieder eine ganze Zahl.*

Beweis. Die Summe oder Differenz zweier ganzer Zahlen α, β:

$$\alpha = a + b\omega$$
$$\beta = c + d\omega,$$

ist

$$\alpha \pm \beta = a \pm c + (b \pm d)\omega,$$

und diese Zahl genügt offenbar den Bedingungen der ganzen Zahlen ebenso wie α und β selbst.

Für das Produkt zweier Zahlen hat man zwei Fälle zu unterscheiden:

1. $m \equiv 1, (4)$; dann ist $\alpha \cdot \beta = ac + (ad + bc)\omega + bd\omega^2$

und da

$$\omega^2 = \frac{1 + 2\sqrt{m} + m}{4} = \frac{m-1}{4} + \omega$$

wird, so ist $\alpha \cdot \beta$ ebenfalls von der Form $u + v\omega$, wo u und v ganze rationale Zahlen bedeuten, und somit eine ganze Zahl.

2. $m \not\equiv 1, (4)$; dann ist $\alpha \cdot \beta = ac + bdm + (ad + bc)\omega$,

also ist $\alpha \cdot \beta$ wieder von der Form $u + v\omega$ und folglich ganz.

Hat man beliebig viele ganze Zahlen $\alpha, \beta, \gamma, \ldots$ und wendet auf dieselben die Operationen der Addition, Subtraktion, Multiplikation beliebig oft nacheinander an, so erhält man immer wieder ganze Zahlen, was man auch folgendermaßen ausdrücken kann:

Satz. *Jede rationale ganze Funktion von ganzen Zahlen $\alpha, \beta, \gamma, \ldots$ des Körpers $k(\sqrt{m})$ mit ganzen rationalen Zahlenkoeffizienten ist wieder eine ganze Zahl des Körpers.*

Wegen ihrer vielfachen Verwendung in den folgenden Sätzen ist es praktisch, einige Begriffe und Benennungen hier einzuführen:

Norm einer Zahl α: $n(\alpha)$ heißt das Produkt der Zahl α mit ihrer Konjugierten α', also

$$n(\alpha) = \alpha \cdot \alpha'.$$

Die Norm einer ganzen Zahl von $k(\sqrt{m})$ ist eine rationale und folglich rationale ganze Zahl, sie ist nâmlich einfach gleich dem Absolutglied der quadratischen Gleichung, welcher α genügt.

Für ein Produkt aus irgend welchen Faktoren berechnet man die Norm nach folgendem Satz:

Satz. *Die Norm des Produkts zweier Zahlen α und β ist gleich dem Produkt der Normen der beiden Zahlen.*

Es ist:

$$n(\alpha\beta) = \alpha\beta \cdot \alpha'\beta' = \alpha\alpha' \cdot \beta\beta' = n(\alpha) \cdot n(\beta).$$

Diskriminante einer Zahl α: $d(\alpha)$ heißt der Ausdruck:

$$d(\alpha) = (\alpha - \alpha')^2,$$

auch diese Zahl ist rational und ganz. Die Diskriminante einer rationalen Zahl ist stets gleich Null.

Diskriminante des Körpers $k(\sqrt{m})$ heißt der Ausdruck:

$$d = d(\omega) = (\omega - \omega')^2.$$

Man kann die Körperdiskriminante in Determinantenform schreiben:

$$d = \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2,$$

und sieht dann leicht, daß, wenn ω_1, ω_2 irgend zwei andere Basiszahlen sind, man auch

$$d = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2$$

setzen kann.

Wenn nämlich

$$\omega_1 = a_1 + b_1\omega, \quad \omega_1' = a_1 + b_1\omega'$$
$$\omega_2 = a_2 + b_2\omega, \quad \omega_2' = a_2 + b_2\omega'$$

gesetzt wird, so muß $\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \pm 1$ sein, und man hat nach dem Multiplikationssatz für Determinanten:

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix} = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix},$$

also, wenn $a_1 b_2 - a_2 b_1 = \pm 1$ ersetzt wird:

$$d = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2 = \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2.$$

Die Diskriminante des Körpers $k(\sqrt{m})$ ist:

$$1.\quad d = m,\quad \text{wenn}\quad m \equiv 1, (4),$$
$$2.\quad d = 4m,\quad \text{wenn}\quad m \not\equiv 1, (4).$$

Die Diskriminante d ist positiv für reelle und negativ für imaginäre Körper. Sie ist nur ungerade, wenn $m \equiv 1$, (4) ist.

Beispiele. Zur Erläuterung der bisher entwickelten Begriffe und Sätze führen wir eine Reihe von Zahlenbeispielen an.

Die Zahl m soll nach unserer Voraussetzung keinen quadratischen Faktor enthalten. Man kann darnach nehmen:

$$m = \pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \pm 11, \pm 13, \ldots$$

Der Körper $k(\sqrt{1})$ ist offenbar der Körper der rationalen Zahlen, der hier nicht für sich untersucht werden soll.

1. Beispiel: $k(\sqrt{-1})$.

Es ist $m = -1$, $m \equiv 3$, (4).

Eine Basis des Körpers bilden 1, $\omega = \sqrt{-1}$.

Die ganzen Zahlen sind enthalten in der Form $a + b\sqrt{-1}$.

Zu einer Zahl $\alpha = a + b\sqrt{-1}$ ist die Konjugierte $\alpha' = a - b\sqrt{-1}$, und es ist die Norm $n(\alpha) = a^2 + b^2$.

Diskriminante einer ganzen Zahl α des Körpers ist $d(\alpha) = -4b^2$.

Eine Ausnahmestellung unter den ganzen Zahlen des Körpers nimmt die Zahl $\varepsilon = \sqrt{-1}$ ein. Für sie ist $n(\varepsilon) = +1$, es ist also $\frac{1}{\varepsilon}$ wieder eine ganze Zahl, und man kann etwa sagen, daß $\sqrt{-1}$ eine ganze Zahl ist, welche in ± 1 aufgeht.

Die Diskriminante des Körpers ist $d = -4$.

Die Basis des Körpers kann aber auch anders dargestellt werden als durch 1, $\sqrt{-1}$, z. B. durch:

$$\omega_1 = 1 + \sqrt{-1}\ (= 1 \cdot 1 + 1\omega),\quad \omega_2 = 2 + \sqrt{-1}\ (= 2 \cdot 1 + 1 \cdot \omega),$$

weil hier

$$a_1 b_2 - a_2 b_1 = -1$$

ist, oder durch

$$\omega_1 = 1 - \sqrt{-1},\quad \omega_2 = -2 + 3\sqrt{-1},$$

wo

$$a_1 b_2 - a_2 b_1 = 1 \text{ ist, usw.}$$

2. Beispiel: $k(\sqrt{5})$.

Es ist $m = 5$, $m \equiv 1$, (4).

Eine Basis des Körpers bilden die Zahlen: 1, $\omega = \frac{1+\sqrt{5}}{2}$; oder 1, ω', weil $\omega' = 1 - \omega$; oder $2 + 3\omega$, $1 + 2\omega$ usw.

Die ganzen Zahlen sind enthalten in der Form $a + b\omega = a + b\frac{1+\sqrt{5}}{2}$.

Zu einer Zahl $\alpha = a + b\omega$ ist die Konjugierte $a + b\omega' = a + b\frac{1-\sqrt{5}}{2}$, und es ist $n(\alpha) = a^2 + ab - b^2$.

Diskriminante $d(\alpha) = 5b^2$.

Wie im vorigen Beispiel des Körpers $k(\sqrt{-1})$ die Zahl $\sqrt{-1}$, so nimmt jetzt die Zahl ω eine Ausnahmestellung unter den ganzen Zahlen des Körpers ein. Es ist nämlich $n(\omega) = -1$ und es geht daher ω oder ω' in ± 1 auf. Ebenso verhalten sich die Zahlen ω^2, $\omega^3 \ldots$, ω^{-1}, ω^{-2}, $\omega^{-3} \ldots$, welche alle untereinander und von ω verschieden sind.

Die Diskriminante des Körpers ist $d = 5$.

Für einige andere Körper stellen wir die Resultate in einer kleinen Tabelle zusammen, indem wir übrigens auf die Tabellen am Schluß des Buches verweisen.

Körper	Charakter von m	Basis	Ganze Zahlen	$n(\alpha)$	$d(\alpha)$	d
$k(\sqrt{5})$	$5 \equiv 1, (4)$	$1, \frac{1+\sqrt{5}}{2}$	$a+b\frac{1+\sqrt{5}}{2}$	a^2+ab-b^2	$5b^2$	5
$k(\sqrt{3})$	$3 \equiv 3, (4)$	$1, \sqrt{3}$	$a+b\sqrt{3}$	a^2-3b^2	$12b^2$	12
$k(\sqrt{2})$	$2 \equiv 2, (4)$	$1, \sqrt{2}$	$a+b\sqrt{2}$	a^2-2b^2	$8b^2$	8
$k(\sqrt{-1})$	$-1 \equiv 3, (4)$	$1, \sqrt{-1}$	$a+b\sqrt{-1}$	a^2+b^2	$-4b^2$	-4
$k(\sqrt{-2})$	$-2 \equiv 2, (4)$	$1, \sqrt{-2}$	$a+b\sqrt{-2}$	a^2+2b^2	$-8b^2$	-8
$k(\sqrt{-3})$	$-3 \equiv 1, (4)$	$1, \frac{1+\sqrt{-3}}{2}$	$a+b\frac{1+\sqrt{-3}}{2}$	a^2+ab+b^2	$-3b^2$	-3

Aus dieser Tabelle ersieht man, daß die Diskriminante eines Körpers jedesmal der größte gemeinsame Teiler aller Diskriminanten der ganzen Zahlen des Körpers ist. Die Diskriminanten der rationalen Zahlen, und nur diese, sind gleich Null.

Die Norm einer ganzen Zahl ist für einen reellen Körper positiv oder negativ, für einen imaginären Körper stets und nur positiv. Jedenfalls ist aber der absolute Betrag der Norm einer ganzen von Null verschiedenen Zahl des Körpers ≥ 1.

7. Teilbarkeit der ganzen Zahlen.

Eine ganze Zahl α des Zahlkörpers $k(\sqrt{m})$ heißt durch eine andere ganze Zahl β dieses Körpers teilbar, wenn man eine ganze Zahl γ so finden kann, daß

$$\alpha = \beta\gamma$$

ist.

Ist eine, in ± 1 nicht aufgehende, ganze Zahl π nur durch sich selbst und durch solche ganze Zahlen teilbar, welche auch in 1 aufgehen, so hat π scheinbar den Charakter der rationalen ganzen Primzahlen und soll vorläufig *unzerlegbar* heißen.

Wenn man nun die Zerlegung irgend einer Zahl in unzerlegbare Faktoren durchgeführt hat, so erhebt sich vor allem die Frage, ob diese Zerlegung auch nur auf *eine* Weise ausgeführt werden kann, oder ob etwa Gleichungen bestehen von der Form:

$$\alpha = \varkappa_1 \cdot \varkappa_2 \cdot \varkappa_3 \ldots \varkappa_n = \pi_1 \cdot \pi_2 \ldots \pi_m,$$

worin die einzelnen $\varkappa$ von den π sich nicht bloß um Faktoren unterscheiden, die in 1 aufgehen, sondern so beschaffen sind, daß kein $\varkappa$ durch irgend eine der Zahlen π teilbar ist.

Man wird versuchen, das Euklidische Teilerverfahren auf die quadratischen Zahlen zu übertragen. Wenn dieser Versuch gelänge, so müßte daraus der Satz von der eindeutigen Zerlegbarkeit folgen. Läßt sich indessen zeigen, daß das Euklidische Teilerverfahren im allgemeinen nicht mehr gilt, so bleibt die Gültigkeit der eindeutigen Zerlegbarkeit zweifelhaft.

Der Deutlichkeit wegen nehmen wir zuerst ein Beispiel durch, und zwar zunächst ein solches, in dem das Verfahren noch gilt: die Zerlegung der ganzen Zahlen im Körper $k(\sqrt{-1})$.

Es seien:

$$\alpha = a_1 + a_2\sqrt{-1}, \quad \beta = b_1 + b_2\sqrt{-1},$$

zwei ganze Zahlen, und zwar $n(\alpha) \geqq n(\beta)$, ohne daß β in α aufgehe, dann soll der größte gemeinsame Teiler von α und β gesucht werden. Die einfache Division $\frac{\alpha}{\beta}$ ergibt eine ganze Zahl und einen Rest:

$$\frac{\alpha}{\beta} = \frac{\alpha\beta'}{n(\beta)} = \gamma + \frac{r + s\sqrt{-1}}{n(\beta)},$$

aber dieser Ansatz ist insofern noch unbestimmt, als r und s zwischen 0 und $n(\beta)$, oder zwischen 0 und $-n(\beta)$, oder endlich zwischen $-\frac{1}{2}n(\beta)$ und $+\frac{1}{2}n(\beta)$ liegen können. Wir setzen fest, daß als Rest „*der absolut kleinste Rest*" genommen werde, indem:

$$|r| \leqq \tfrac{1}{2} n(\beta) \quad \text{und} \quad |s| \leqq \tfrac{1}{2} n(\beta)$$

zu wählen ist. Dann kann man die Division $\alpha : \beta$ so ansetzen:

$$\alpha = \gamma \beta + \varrho_0,$$

wo $\varrho_0 = \frac{r + s\sqrt{-1}}{\beta'}$ nun eine ganze Zahl ist, für welche

$$n(\varrho_0) = \frac{r^2 + s^2}{n(\beta')} \leqq \tfrac{1}{2} n(\beta)$$

wird.

Ist $n(\varrho_0) > 1$, so dividiere man jetzt β durch ϱ_0, und zwar sei

$$\beta = \gamma_1 \varrho_0 + \varrho_1,$$

indem nun neuerdings ϱ_1 so gewählt ist, daß:

$$n(\varrho_1) \leqq \tfrac{1}{2} n(\varrho_0),$$

ausfällt und setze diese Division so lange fort, bis einmal $n(\varrho_{n-1}) > 1$ und entweder $n(\varrho_n) = 0$, oder $n(\varrho_n) = 1$ wird. Eine dieser beiden Möglichkeiten muß einmal eintreten, weil die Normen der Reste eine abnehmende Reihe von positiven ganzen rationalen Zahlen bilden.

Im ersten Fall ist $\varrho_n = 0$, und es sind α und β durch ϱ_{n-1} teilbar; im zweiten Fall, wo $n(\varrho_n) = 1$ ist, geht ϱ_n offenbar in 1 auf und es sind α und β nur durch 1 oder eine in 1 aufgehende Zahl teilbar, also teilerfremd.

Nach dieser Betrachtung gilt für die Zahlen des Körpers $k(\sqrt{-1})$ das Euklidische Teilerverfahren, da die Rechnung nach einer *endlichen* Anzahl von Schritten abbrechen muß, und darum gilt auch noch der Satz von der eindeutigen Zerlegung der ganzen Zahlen in Primfaktoren.

Nun betrachten wir den allgemeineren Fall $k(\sqrt{m})$, wenn $m \not\equiv 1, (4)$ ist. Indem wir zwei Zahlen $\alpha : \beta$ dividieren nach dem Schema:

$$\frac{\alpha}{\beta} = \frac{\alpha \cdot \beta'}{n(\beta)} = \gamma + \frac{r + s\sqrt{m}}{n(\beta)},$$

oder

$$\alpha = \gamma \beta + \varrho_0,$$

können wir wiederum annehmen[1]):

$$|r| \leqq \tfrac{1}{2} |n(\beta)|, \quad |s| \leqq \tfrac{1}{2} |n(\beta)|,$$

dann ist:

$$n(\varrho_0) = \frac{r^2 - s^2 m}{n(\beta')},$$

also

1) Dieser so gewählte Rest der Division soll wieder *„der absolut kleinste Rest"* nach β heißen.

$$|n(\varrho_0)| \leqq |n(\beta)| \left|\frac{1}{4} - \frac{m}{4}\right|.$$

Aus dieser Ungleichung folgt nun weiter die allgemeine Ungleichung

$$|n(\varrho_0)| < |n(\beta)|$$

nur dann, wenn $3 > m > -3$ ist. In allen andern Fällen *kann* eintreten, daß $|n(\varrho_0)| > |n(\beta)|$ usw. wird, dann braucht das Verfahren nicht mehr nach einer endlichen Anzahl von Schritten abzubrechen, und dieser Fall ist der allgemeine für die Zahlen des allgemeinen Körpers $k(\sqrt{m})$. Natürlich ist darum für diese Körper der Satz von der eindeutigen Zerlegung nicht mehr auf das Euklidische Teilerverfahren zu gründen, und es bleibt seine Gültigkeit überhaupt zweifelhaft.

Ein gleiches ergibt sich für die Körper $k(\sqrt{m})$, wenn $m \equiv 1, (4)$ ist.

Tatsächlich zeigen auch direkt die folgenden speziellen Beispiele, daß es Körper gibt, deren Zahlen in mehrfacher Weise in Faktoren zerlegt werden können, in denen also der Fundamentalsatz der rationalen Zahlentheorie *nicht* mehr gilt.

1. Beispiel. Der zu betrachtende Körper sei $k(\sqrt{-5})$.

Die ganzen Zahlen desselben sind von der Form:

$$a + b\sqrt{-5}.$$

Die einzigen ganzen Zahlen des Körpers, welche in der Zahl 1 aufgehen, oder deren Norm $+1$ ist, sind ± 1. Denn ist:

$$1 = (a + b\sqrt{-5})(a_1 + b_1\sqrt{-5}),$$

so folgt durch Übergang zu den Normen:

$$1 = (a^2 + 5b^2)(a_1 + 5b_1^2),$$

und da die Normen rechts ganze Zahlen sind, so bleibt nur:

$$1 = a^2 + 5b^2 = a_1^2 + 5b_1^2$$

mit der Lösung $a = a_1 = \pm 1$, $b = b_1 = 0$ übrig.

Untersucht man nun die Zahl 21, so findet man die Zerlegungen:

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

wo jetzt die ganzen Zahlen

$$3,\ 7,\ 4 + \sqrt{-5},\ 4 - \sqrt{-5},\ 1 + 2\sqrt{-5},\ 1 - 2\sqrt{-5}$$

lauter unzerlegbare Zahlen sind, die alle wesentlich verschieden voneinander sind.

Wäre z. B. 3 zerlegbar, so hätte man etwa:

$$3 = (a + b\sqrt{-5})(a_1 + b_1\sqrt{-5}),$$

woraus durch Ausmultiplizieren und Vergleich beider Seiten der Gleichung sich ergibt:

$$3 = aa_1 - 5bb_1$$
$$0 = ab_1 + a_1 b.$$

Die letzte Relation ergibt, unter P einen noch unbekannten von Null verschiedenen Proportionalitätsfaktor verstanden:

$$a_1 = P \cdot a, \quad b_1 = - P \cdot b,$$

also folgt aus der ersten Gleichung:

$$3 = Pa^2 + 5Pb^2,$$

wo Pa^2 und Pb^2 positive ganze Zahlen sind. Falls $b \neq 0$, so wäre $5Pb^2 > 3$, also könnte die letzte Gleichung nicht bestehen, und es ergibt sich als einzig mögliche Lösung:

$$3 = Pa^2, \quad 0 = Pb^2,$$

oder:

$$\begin{cases} b = 0, & a = 3, \quad P = \frac{1}{3} \text{ und} \\ b_1 = 0, & a_1 = 1 \end{cases}$$

bezw.

$$\begin{cases} b = 0, & a = 1, \quad P = 3 \text{ und} \\ b_1 = 0, & a_1 = 3 \end{cases}$$

d. h. man erhält $3 = 3 \cdot 1 = 1 \cdot 3$, also ist 3 unzerlegbar.

Wäre $4 + \sqrt{-5}$ zerlegbar, etwa in der Form:

$$4 + \sqrt{-5} = (a + b\sqrt{-5})(a_1 + b_1\sqrt{-5}),$$

so erhielte man durch Bildung der Normen rechts und links:

$$21 = (a^2 + 5b^2)(a_1^2 + 5b_1^2),$$

und da man in dieser Gleichung nur ganze rationale Zahlen hat, so bleiben folgende Möglichkeiten:

1. $\quad 21 = a^2 + 5b^2, \quad 1 = a_1^2 + 5b_1^2$

mit den schon bekannten Lösungen:

1a. $\quad a = 4, \quad b = 1, \quad a_1 = \pm 1, \quad b_1 = 0,$

und der, die ursprüngliche Gleichung nicht befriedigenden Lösung

1b. $\quad a = 1, \quad b = 2, \quad a_1 = \pm 1, \quad b_1 = 0.$

2. $\quad 3 = a^2 + 5b^2, \quad 7 = a_1^2 + 5b_1^2$

ohne Lösungen, und:

3. $\quad 3 = a_1^2 + 5b_1^2, \quad 7 = a^2 + 5b^2$

ohne Lösung. Ganz ebenso zeigt sich, daß 7, $1 + 2\sqrt{-5}$, $1 - 2\sqrt{-5}$ unzerlegbar sind.

Es bleibt nur noch nachzuweisen, daß die drei Zerlegungen auch wesentlich verschieden sind und sich nicht nur um Faktoren der 1 unterscheiden. Wäre z. B.

$$4+\sqrt{-5}=(1+2\sqrt{-5})(x+y\sqrt{-5}),$$

so folgt:

$$4=x-10y$$

$$1=2x+y,$$

woraus man berechnet:

$$x=\tfrac{2}{3},\quad y=-\tfrac{1}{3},$$

daher ist $4+\sqrt{-5}$ durch $1+2\sqrt{-5}$ nicht teilbar, und ähnliches läßt sich für die übrigen Möglichkeiten beweisen.

Einfachere Zerlegungen im selben Zahlenkörper sind z. B.:

$$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5}),$$
$$9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5}) \text{ etc.}$$

Dieses Beispiel zeigt klar, daß es Zahlen gibt, welche sich auf ganz verschiedene Weisen in Faktoren zerlegen lassen können. Der Begriff der „unzerlegbaren" Zahl deckt sich ganz und gar nicht mit dem uns geläufigen Begriff der rationalen Primzahl.

2. Beispiel. Wir betrachten jetzt den *reellen* Zahlkörper $k(\sqrt{10})$.

Da $10\equiv 2, (4)$ ist, so sind die ganzen Zahlen von der Form:

$$a+b\sqrt{10}.$$

Zunächst interessieren die ganzen Zahlen des Körpers, welche in ± 1 aufgehen. Wenn ε eine solche Zahl ist, und $\pm 1=\varepsilon\cdot\varepsilon_1$ gesetzt wird, so ist $1=n(\varepsilon)\cdot n(\varepsilon_1)$. Da die Norm einer ganzen Zahl selbst eine ganze rationale Zahl ist, so hat man $n(\varepsilon)=\pm 1$ und $n(\varepsilon_1)=\pm 1$ zu setzen. Man kann daher gleichbedeutend füreinander sagen, entweder eine ganze Zahl geht in 1 auf, oder die Norm einer ganzen Zahl sei ± 1. Setzt man $\varepsilon=a+b\sqrt{10}$, so haben wir also die Werte a, b zu bestimmen, für welche: $\pm 1=a^2-10b^2$ ist.

Durch einfaches Probieren findet man für die Gleichung

$$-1=a^2-10b^2$$

sofort eine Lösung:

$$a=\pm 3,\quad b=\pm 1,$$

und man hat

$$-1=(3+\sqrt{10})(3-\sqrt{10}),$$

oder

$$-1=(-3+\sqrt{10})(-3-\sqrt{10}).$$

Aus diesen Gleichungen lassen sich aber dann unendlich viele weitere Lösungen der ursprünglichen Gleichung ableiten.

Durch Quadrieren erhält man nämlich:

$$1 = (19 + 6\sqrt{10})(19 - 6\sqrt{10}),$$

und diese Zerlegung enthält für die Gleichung

$$1 = a^2 - 10b^2$$

die weitere Lösung $a = 19$, $b = 6$.

Auf analoge Weise liefert jede ganzzahlige Potenz:

$$(-1)^e = (3 + \sqrt{10})^e (3 - \sqrt{10})^e$$

eine Lösung der Gleichung:

$$(-1)^e = a^2 - 10b^2.$$

Durch diese Zahlen $3 + \sqrt{10}$, $-3 + \sqrt{10}$, $19 + 6\sqrt{10}$ usw. ist aber natürlich nicht nur die Zahl 1, sondern *jede* ganze Zahl des Körpers teilbar.

Wir werden nun zwei Zerlegungen einer Zahl wie z. B.

$$6 = 2 \cdot 3$$

und

$$6 = -2 \cdot 3(3 + \sqrt{10})(3 - \sqrt{10})$$

nicht als wesentlich verschieden betrachten, sondern nur als *eine* Zerlegung ansehen.

Mit dieser Beschränkung sind 2 und 3 unzerlegbar. Die Zerlegung

$$-4 = (6 + 2\sqrt{10})(6 - 2\sqrt{10})$$

ist nicht wesentlich verschieden von der Zerlegung $4 = 2 \cdot 2$.

Dagegen ist

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$$

eine doppelte Zerlegung der Zahl 6, während die Zerlegungen

$$6 = (4 + \sqrt{10})(4 - \sqrt{10})$$

und

$$6 = (16 + 5\sqrt{10})(16 - 5\sqrt{10})$$

gleich sind, weil die Zahlen $4 + \sqrt{10}$ und $16 - 5\sqrt{10}$ einerseits, $4 - \sqrt{10}$ und $16 + 5\sqrt{10}$ andererseits sich nur um einen in 1 aufgehenden Faktor unterscheiden, indem z. B.

$$(4 + \sqrt{10})(19 - 6\sqrt{10}) = 16 - 5\sqrt{10}$$

ist.

Dieser Fall zeigt, daß wegen der in 1 aufgehenden ganzen Zahlen in einem reellen Körper zwei sehr verschieden aussehende Zerlegungen doch wesentlich gleich sein können. Es bleibt jedoch die Tatsache der mehrfach möglichen Zerlegung der Zahl 6 im Körper $k(\sqrt{10})$ bestehen, und dasselbe ließe sich für beliebig viele andere Zahlen nachweisen.

Wenn aber schon in speziellen Fällen der Satz von der eindeutigen Zerlegung einer ganzen Zahl des Körpers $k(\sqrt{m})$ in unzerlegbare Faktoren nicht mehr gilt, so ist an einen Beweis des Satzes im allgemeinen überhaupt nicht zu denken. Die Theorie hat sich mit der zwei- und mehrfach möglichen Zerlegung einer ganzen Zahl in Faktoren abzufinden. Damit werden aber auch alle die schönen Gesetze der rationalen Zahlentheorie hinfällig. Mit dieser Tatsache würde eine Zahlentheorie der algebraischen Zahlen ungeheuer schwerfällig, wo nicht unmöglich werden.

Nachdem mehrere Mathematiker (Gauß, Kummer 1844) diesen Übelstand bemerkt hatten, fand Kummer auch einen Ausweg aus den entstandenen Schwierigkeiten. Um den Satz von der eindeutigen Zerlegbarkeit für die algebraischen Zahlen wieder herzustellen, führte er[1]) den Begriff der *Idealzahlen* ein. Man darf die Entdeckung dieses Begriffes zu den schönsten Entdeckungen in der Zahlentheorie zählen. Es wäre reizvoll, die Darstellung der Idealzahlen nach Kummer hier anzuführen, doch muß ich darauf verzichten und will mich gleich zu dem Begriff der *Ideale* wenden, den Herr Dedekind[2]) aus dem Begriff der Idealzahlen in glücklicher Weise entwickelte, da er dadurch dem ursprünglichen Begriff eine realere Existenz gab.

8. Spezielle Zahlsysteme und Ideale.

Der Begriff des Ideals läßt sich sehr deutlich entwickeln an einem ganz speziellen Fall. Betrachtet man nicht den vollen Bereich der ganzen rationalen Zahlen, sondern nur einen Teil desselben, z. B.

---

1) Crelles Journal, Bd. 35, S. 319: Zur Theorie der komplexen Zahlen, und ibid. S. 327: Über die Zerlegung der aus Wurzeln der Einheit gebildeten komplexen Zahlen in ihre Primfaktoren. Die Entwicklungen von Kummer beziehen sich auf den sogenannten Kreiskörper. (Ber. der k. Akad. Berlin, März 1845.)

Die Idealzahlen hat P. Bachmann in seiner Zahlentheorie, Bd. V, S. 144 für den quadrat. Körper erläutert.

2) Vorles., Suppl. XI, p. 550 (Modul S. 493).

die Gesamtheit[1]) der Zahlen von der Form $4n + 1$, so kann man das Produkt irgend zweier Zahlen bilden und die Division wie üblich definieren, während von der Addition und Subtraktion abgesehen werden soll. In der Reihe:

$$1,\ 5,\ 9,\ 13,\ 17,\ 21,\ 25\ \ldots\ 73,\ 77\ \ldots\ 141\ \ldots$$

steckt offenbar das Produkt irgend zweier Zahlen wieder drin, denn es ist:

$$(4n + 1)(4n_1 + 1) = 4m + 1,$$

$$(\text{Beisp.}\quad 5 \cdot 9 = 45,\quad 9 \cdot 13 = 117\ \text{usw.})$$

und man darf in einem Produkt auch die Faktoren vertauschen.

Die Zahlen 5, 9, 13, 17, 21, 29 ... sind unzerlegbar in dem zugrunde gelegten Zahlbereich. Nimmt man z. B. 21, so ist diese Zahl nicht gleich dem Produkt zweier anderer Zahlen der Reihe. Die Zahl 10857 z. B. läßt dagegen folgende Zerlegungen zu:

$$10857 = 141 \cdot 77 = 21 \cdot 517,$$

und es sind diese Zerlegungen wesentlich verschieden, weil 21, 77, 141, 517 unzerlegbar sind. Ebenso ist:

$$693 = 21 \cdot 33 = 9 \cdot 77$$

$$441 = 21^2 \quad = 9 \cdot 49 \quad \text{usw.}$$

Für uns ist nun aber von vornherein ganz klar, wie diese Zerlegungen eindeutig gemacht werden können. Nimmt man zu den angeschriebenen Zahlen noch alle übrigen ganzen rationalen Zahlen hinzu, so ist doch beispielsweise im ersten Fall:

$$10857 = 3 \cdot 7 \cdot 11 \cdot 47$$

eine eindeutige Zerlegung in dem vollen erweiterten Bereich. Der Gedanke von Kummer besteht nun, auf den Spezialfall angewendet, darin, diese elementaren Faktoren 3, 7, 11, 47 als *Idealzahlen* den Zahlen des Körpers zu adjungieren. Die Zahl 3 kann ja angesehen werden als größter gemeinsamer Teiler von 21 und 141; 7 desgl. von 77 und 21; 11 desgl. von 77 und 517; 47 desgl. von 141 und 517. Bezeichnet man nun mit dem *Symbol*

$$\textit{Ideal}\ \mathfrak{j} = (a, b)$$

nichts anderes als eben den größten gemeinsamen Teiler der beiden ganzen Zahlen a und b, so wird in dem behandelten Beispiel der Faktor 3 identisch mit dem Symbol (21, 141), ferner 7 identisch mit

1) Herr Fueter nennt ein ähnliches derartiges System „Zahlstrahl", siehe Crelles Journal, Bd. 130, S. 208.

(21, 77) und 11 resp. 47 identisch mit (77, 517) bez. (141, 517). Nehmen wir nun noch das Symbol $\mathfrak{j} = (a)$ hinzu, so kann man schreiben:

$$(141) = (21, 141)(141, 517); \quad (77) = (21, 77)(77, 517)$$

und

$$(10857) = (21, 141)(141, 517)(77, 21)(77, 517).$$

Weil andererseits

$$(21) = (21, 141)(21, 77); \quad (517) = (517, 77)(517, 141)$$

ist, so geben $141 \cdot 77$ und $21 \cdot 517$ dieselben Zerlegungen. Ganz analog erhält man in den beiden anderen Beispielen:

$$(693) = (21, 9)(21, 77)(33, 9)(33, 77),$$
$$(441) = (21, 9)(21, 49)(21, 9)(21, 49).$$

An diese Einführung der Symbole (a, b) schließen sich folgende leicht einzusehende Folgerungen:

Das Symbol (a, b) ändert sich nicht, wenn man demselben irgend eine Zahl beifügt von der Form:

$$ac + bd,$$

wo c und d beliebige, dem System angehörige Zahlen sind, d. h. die Symbole:

$$(a, b)$$

und

$$(a, b, ac + bd)$$

stellen dasselbe Ideal vor. Es kann daher ebenso gut ein Ideal definiert werden als ein Simultansystem von *beliebig vielen* Zahlen, d. h. als der größte gemeinsame Teiler derselben, und man hat nur ein Kriterium für die Gleichheit irgend zweier gegebener Ideale zu entwickeln. In dem Zahlenbeispiel ergibt sich sofort:

Zwei Ideale sind gleich, wenn jede Zahl des einen Ideals auch in dem zweiten Ideal vorkommt, oder durch eine lineare Kombination der Zahlen des zweiten Ideals mit geeigneten Zahlen des gegebenen Zahlsystems erzeugt werden kann.

Wir wenden uns jetzt zum allgemeinen Fall.

9. Die Ideale des quadratischen Zahlkörpers.

Man nimmt zu den ganzen Zahlen eines Körpers von Anfang an unendlich viele *Ideale* hinzu, welche folgendermaßen definiert sind:

Definition. *Ein System von ganzen Zahlen des Körpers* $k(\sqrt{m})$: $\mathfrak{j} = (\alpha, \beta, \gamma, \ldots)$ *von der Beschaffenheit, daß jede lineare Kombination:*

$$\alpha\lambda + \beta\mu + \gamma\nu + \cdots$$

der Zahlen $\alpha, \beta, \gamma \ldots$ *mit ganzen Zahlen* $\lambda, \mu, \nu \ldots$ *des Körpers wiederum dem System angehört, heißt ein Ideal des Körpers.*

Insbesondere heißt ein Ideal *Hauptideal*, wenn seine Zahlen die Vielfachen einer dem Ideal angehörigen ganzen Zahl des Körpers sind, d. h. wenn es die Form besitzt: $\mathfrak{j} = (\alpha, \alpha\lambda, \alpha\mu, \ldots)$. Man schreibt alsdann einfach $\mathfrak{j} = (\alpha)$.

Es ist künftig genau zu unterscheiden zwischen Idealen, Hauptidealen und Zahlen, doch kann man wohl oft ohne Zweideutigkeit Zahlen statt der Hauptideale u. v. v. setzen.

Ideale, welche nicht Hauptideale sind, heißen häufig *Nebenideale*, wir wollen sie *Nicht-Hauptideale* nennen.

Enthält ein Ideal $\mathfrak{j}$ die 1 oder eine in 1 aufgehende ganze Zahl, so ist es ein *Einheitsideal* und wird symbolisch $\mathfrak{j} = (1)$ geschrieben.

Bezüglich der *Bezeichnung* setzen wir fest, daß Ideale stets mit deutschen Buchstaben $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots \mathfrak{p} \ldots$ benannt werden sollen.

Um überhaupt mit diesen neuen Symbolen operieren zu können, ist erforderlich, daß man ein Kriterium für die Gleichheit, resp. Verschiedenheit, zweier Ideale hat und die für irgend zwei Ideale möglichen Verknüpfungen (Multiplikation und Division) festlegt.

Für die Gleichheit zweier Ideale sei festgesetzt:

Definition. *Zwei Ideale* $(\alpha, \beta, \gamma \ldots)$ *und* $(\alpha_1, \beta_1, \gamma_1 \ldots)$ *des Körpers* $k(\sqrt{m})$ *sind gleich, in Zeichen ausgedrückt, es ist:*

$$(\alpha, \beta, \gamma \ldots) = (\alpha_1, \beta_1, \gamma_1 \ldots),$$

wenn jede Zahl α *des ersten Ideals auch dem zweiten Ideal angehört (ev. durch eine lineare Kombination* $\alpha_1\lambda + \beta_1\mu + \cdots$ *erzeugt werden kann) und umgekehrt, wenn jedes* α_1, β_1 *usf. auch dem ersten Ideal angehört.*

Für die *Multiplikation* der Ideale soll die folgende Festsetzung gelten:

Sind $\mathfrak{a} = (\alpha, \beta, \gamma \ldots)$ *und* $\mathfrak{b} = (\alpha_1, \beta_1, \gamma_1 \ldots)$ *zwei Ideale des Körpers* $k(\sqrt{m})$, *so versteht man unter dem Produkt derselben dasjenige Ideal, welches gebildet wird aus allen Zahlen, welche man erhält, wenn man jede Zahl aus* $\mathfrak{a}$ *mit jeder Zahl aus* $\mathfrak{b}$ *multipliziert und diesem System noch alle linearen Kombinationen dieser Produkte mit ganzen Zahlen des Körpers hinzufügt:*

$$\mathfrak{a}\mathfrak{b} = (\alpha\alpha_1, \alpha\beta_1, \alpha\gamma_1, \alpha_1\beta, \beta\beta_1, \ldots \gamma\gamma_1 \ldots).$$

Aus der Definition folgt unmittelbar die Vertauschbarkeit der Faktoren: $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, und ferner ergibt sich für die *Division*:

Ein Ideal $\mathfrak{a}$ *ist durch ein Ideal* $\mathfrak{b}$ *teilbar, wenn man ein Ideal* $\mathfrak{c}$ *des Körpers angeben kann, so daß*

$$\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$$

ist. $\mathfrak{c}$ heißt der Quotient der Ideale $\mathfrak{a}$ und $\mathfrak{b}$.

Während die Multiplikation und Divison von den ganzen Zahlen auf die Ideale ausdehnbar ist, so läßt sich dagegen der Begriff der Addition resp. Subtraktion auf die Ideale nicht erweitern, es bleibt diese Verknüpfung auf die Zahlen beschränkt.

Satz. *In jedem Ideal des Körpers* $k(\sqrt{m})$ *lassen sich unendlich vielmal zwei ganze Zahlen des Körpers* ι_1^* *und* ι_2^* *so angeben, daß jede Zahl des Ideals sich als lineare Kombination dieser beiden mit ganzen rationalen Koeffizienten* l_1 *und* l_2 *in der Form:*

$$l_1 \iota_1^* + l_2 \iota_2^*$$

darstellen läßt.

Beweis. Wir schreiben das Ideal $\mathfrak{j}$ so, daß wir jede Zahl durch die Körperbasis 1, ω ausdrücken:

$$\mathfrak{j} = (a + b\omega,\ a_1 + b_1\omega,\ a_2 + b_2\omega, \ldots A_1 \ldots),$$

und beweisen zunächst: wenn $a + b\omega$ und $a_1 + b_1\omega$ irgend zwei Zahlen des Ideals sind, so gehört dem Ideal auch eine Zahl $a' + b'\omega$ an, in welcher b' der größte gemeinsame Teiler der Zahlen b und b_1 ist. In der Tat gehört ja nach Spezialisierung der früheren Definition dem Ideal auch jede Zahl

$$x(a + b\omega) + y(a_1 + b_1\omega)$$

an, wenn x, y rationale ganze Zahlen bedeuten. Man kann aber x, y so bestimmen, daß die Diophantische Gleichung:

$$xb + yb_1 = b',$$

erfüllt ist, und damit ist die Behauptung erwiesen. Durch wiederholte Anwendung dieser Bemerkung auf $a' + b'\omega$ und $a_2 + b_2\omega$ usf. ergibt sich nun, daß dem Ideal eine Zahl

$$J_1 + i_2\omega$$

angehört, wo i_2 der größte gemeinsame Teiler *aller* Zahlen $b, b_1, b_2 \ldots$ ist, während J_1 eine noch bestimmten Bedingungen genügende ganze rationale Zahl sein muß. Die Zahlen $\frac{b}{i_2}$, $\frac{b_1}{i_2}$ usw. sind lauter ganze rationale Zahlen, woraus folgt, daß auch alle die rationalen ganzen Zahlen

$$a + b\omega - \frac{b}{i_2}(J_1 + i_2\omega) = a - \frac{b}{i_2} J_1 \text{ usf.}$$

dem Ideal angehören. Jedes Ideal enthält somit beliebig viele ratio-

nale ganze Zahlen, wie auch von vornherein einleuchtet, da ja außer einer Zahl α auch $\alpha\alpha' = n(\alpha)$ zu den Zahlen des Ideals gehört. Nun sei i der größte gemeinsame Teiler aller rationalen ganzen Zahlen des Ideals, dann gehört i dem Ideal an, was man mit genau denselben Schlüssen nachweist, wie sie oben für die Zahlen b, b_1 und b' angewendet wurden. Wählt man nun noch die ganze rationale Zahl v so, daß

$$0 \leqq i_1 = J - vi < i$$

wird, so ist auch $J + i_2\omega - vi = i_1 + i_2\omega$ eine Zahl des Ideals, und es sind

$$\iota_1 = i$$

und

$$\iota_2 = i_1 + i_2\omega$$

zwei Zahlen wie sie der Satz verlangt.

Es möge nämlich $\alpha = a + b\omega$ eine *beliebige* Zahl des Ideals sein, so ist $l_2 = \frac{b}{i_2}$ ganz, und dem Ideal gehört auch die Zahl an:

$$\alpha - l_2\iota_2 = a - l_2 i_1,$$

welche ganz und rational ist, folglich wird nach unserer Bestimmung von i:

$$a - l_2 i_1 = l_1 i,$$

wo l_1 eine ganze rationale Zahl bedeutet, und man hat zusammengefaßt:

$$\alpha = l_1 i + l_2\iota_2 = l_1\iota_1 + l_2\iota_2,$$

w. z. b. w.

Man kann sonach das Ideal darstellen in der Form:

$$\mathfrak{j} = (i,\ i_1 + i_2\omega),$$

und diese Darstellung soll künftig die *kanonische* Darstellung heißen.

Wir wollen nun gleich aus der Definition des Ideals noch einige Beziehungen der rationalen Zahlen i, i_1, i_2 ablesen.

Da nämlich für irgend zwei ganze rationale Zahlen x, y die Zahl

$$xi\omega + y(i_1 + i_2\omega) = yi_1 + (xi + yi_2)\omega$$

zum Ideal gehört, und darnach

$$xi + yi_2 \equiv 0, (i_2)$$

ist, so muß i ein Vielfaches von i_2 sein, da ferner

$$\omega'(i_1 + i_2\omega) = i_2\omega\omega' + i_1\omega'$$

zum Ideal gehört, so muß auch i_1 ein Vielfaches von i_2 sein.

Die Norm jeder quadratischen Zahl α, welche dem Ideal angehört, muß durch die Zahl i teilbar sein.

Die Zahlen $\iota_1 = i$, $\iota_2 = i_1 + i_2\omega$, oder allgemein irgend zwei ganze Zahlen ι_1^*, ι_2^* des Ideals, welche den Bedingungen des Satzes genügen, heißen eine *Basis* des Ideals, analog der früher eingeführten Bezeichnung Basis des Körpers.

Aus einer Basis ι_1, ι_2 des Ideals kann man auf unendlich viele Weisen eine andere Basis ι_1^*, ι_2^*:

$$\iota_1^* = a_1\iota_1 + a_2\iota_2$$
$$\iota_2^* = b_1\iota_1 + b_2\iota_2$$

mit den ganzzahligen Koeffizienten a_1, a_2, b_1, b_2 ableiten, indem diese letzteren als ganze rationale Zahlen so gewählt werden, daß $a_1b_2 - a_2b_1 = \pm 1$ ist. Nachdem schon bei der Untersuchung der Körperbasis gezeigt wurde, daß dies auf unendlich viele Weisen geschehen kann, wobei man jedesmal wieder eine andere Basis erhält, ist der Satz in allen Teilen bewiesen.

Für zwei verschiedene Paare von Basiszahlen eines Ideals gilt derselbe Satz (S. 25), wie für Basiszahlen des Körpers.

Beispiele. Wir nehmen zur Erläuterung der eingeführten Begriffe wieder einige Beispiele durch.

1. Beispiel: $k(\sqrt{-5})$.

In diesem schon behandelten Zahlkörper ergab sich u. a.:

$$21 = 3 \cdot 7 = (4+\sqrt{-5})(4-\sqrt{-5}) = (1+2\sqrt{-5})(1-2\sqrt{-5});$$

bilden wir nach Analogie des Zahlenbeispiels S. 36 jetzt die Ideale:

$$(3,\ 4+\sqrt{-5}),\quad (3,\ 4-\sqrt{-5});$$
$$(3,\ 1+2\sqrt{-5}),\quad (3,\ 1-2\sqrt{-5});$$
$$(7,\ 4+\sqrt{-5}),\quad (7,\ 4-\sqrt{-5});$$
$$(7,\ 1+2\sqrt{-5}),\quad (7,\ 1-2\sqrt{-5});$$
$$(4+\sqrt{-5},\ 1+2\sqrt{-5}),\quad (4+\sqrt{-5},\ 1-2\sqrt{-5});$$
$$(4-\sqrt{-5},\ 1+2\sqrt{-5}),\quad (4-\sqrt{-5},\ 1-2\sqrt{-5}),$$

so haben wir hier Ideale, durch welche nun die Zerlegung von 21 eindeutig gemacht werden kann.

Die angeschriebenen Ideale sind nicht alle verschieden voneinander. So überzeugt man sich, daß

$$(3,\ 4+\sqrt{-5}) = (3,\ 1-2\sqrt{-5})$$

ist, denn es ist:

$$3 \cdot 3 - 2(4+\sqrt{-5}) = 1-2\sqrt{-5},$$

also: $$(3,\ 4+\sqrt{-5}) = (3,\ 4+\sqrt{-5},\ 1-2\sqrt{-5}).$$

Ebenso ist:

$$(3,\ 4-\sqrt{-5}) = (3,\ 1+2\sqrt{-5}) = (4-\sqrt{-5},\ 1+2\sqrt{-5})$$
$$(7,\ 4+\sqrt{-5}) = (7,\ 1+2\sqrt{-5}) = (4+\sqrt{-5},\ 1+2\sqrt{-5})$$
$$(7,\ 4-\sqrt{-5}) = (7,\ 1-2\sqrt{-5}) = (4-\sqrt{-5},\ 1-2\sqrt{-5}).$$

Lassen wir uns durch die Analogie mit dem Beispiel des speziellen Zahlensystems leiten, so werden wir nun setzen:

$$(21) = (3,\ 4+\sqrt{-5})(3,\ 4-\sqrt{-5})(7,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5});$$

und dieser Ansatz ist richtig, wie man leicht durch Multiplikation bestätigt. Es ist:

$$(3) = (3,\ 4+\sqrt{-5})(3,\ 4-\sqrt{-5})$$
$$= (9,\ 12+3\sqrt{-5},\ 12-3\sqrt{-5},\ 21,\ 3),$$

weil nämlich die Kombination aus 21 und 9:

$$21 - 2\cdot 9 = 3$$

dem Idealprodukt auch angehört und somit alle Zahlen desselben Vielfache von 3 sind. Geradeso findet sich:

$$(7,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5})$$
$$= (49,\ 28+7\sqrt{-5},\ 28-7\sqrt{-5},\ 21) = (7).$$

Die Ideale $(3,\ 4+\sqrt{-5})$, $(3,\ 4-\sqrt{-5})$ bieten sich in der kanonischen Darstellung dar, wie man leicht sieht. Das Ideal: $(4+\sqrt{-5},\ 1-2\sqrt{-5})$ ist dagegen nicht in der kanonischen Darstellung geschrieben; wir wollen dieselbe (die allerdings schon bekannt ist) aufsuchen.

Es ist:

$$(4+\sqrt{-5},\ 1-2\sqrt{-5}) = (4+\sqrt{-5},\ 1-2\sqrt{-5},\ 21,\ 7\ \ldots).$$

Der größte gemeinschaftliche Faktor aller Koeffizienten von $\sqrt{-5}$ ist offenbar 1, wir können also setzen:

$$\iota_2 = 4+\sqrt{-5},$$

der größte gemeinsame Faktor aller rationalen Zahlen ist

$$\iota_1 = 7,$$

womit die kanonische Darstellung gewonnen ist:

$$(4+\sqrt{-5},\ 1-2\sqrt{-5}) = (7,\ 4+\sqrt{-5}).$$

Durch Ausmultiplizieren von

$$(3,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5}) \quad \text{und}$$

$$(3,\ 4-\sqrt{-5})(7,\ 4+\sqrt{-5})$$

erhält man zwei Ideale:

$$(21,\ 28+7\sqrt{-5},\ 12-3\sqrt{-5})$$
$$(21,\ 28-7\sqrt{-5},\ 12+3\sqrt{-5}),$$

und man erkennt leicht, daß die kanonischen Darstellungen derselben sind:

$$(21,\ 10+\sqrt{-5}),\ \text{resp.}\ (21,\ 10-\sqrt{-5}).$$

Diese Ideale sind Hauptideale, wie man leicht beweist gleich

$$(1-2\sqrt{-5})\ \text{resp.}\ (1+2\sqrt{-5}).$$

Das Ideal (2) zerfällt in $k(\sqrt{-5})$ in das Produkt zweier Nichthauptideale, es ist:

$$(2)=(2,\ 1+\sqrt{-5})(2,\ 1-\sqrt{-5})$$
$$=(4,\ 2+2\sqrt{-5},\ 2-2\sqrt{-5},\ 6,\ 2\ \ldots);$$

da aber

$$(2,\ 1+\sqrt{-5})=(2,\ 1+\sqrt{-5},\ 2-1-\sqrt{-5})$$

ist, so kann man auch schreiben:

$$(2)=(2,\ 1+\sqrt{-5})^2.$$

2. Beispiel: $k(\sqrt{10})$.

Früher hat sich in diesem Körper ergeben:

$$6=2\cdot 3=(4+\sqrt{10})(4-\sqrt{10}).$$

Hieraus leitet man die Ideale ab:

$$(2,\ 4+\sqrt{10})=(2,\ \sqrt{10})=(2,\ 4-\sqrt{10})$$
$$(3,\ 4+\sqrt{10})=(3,\ 1+\sqrt{10})$$
$$(3,\ 4-\sqrt{10})=(3,\ 1-\sqrt{10}),$$

wo jetzt alle diese Ideale schon in kanonischer Darstellung geschrieben sind, und die zwei verschiedenen Zerlegungen werden nun zu einer einzigen eindeutigen Zerlegung:

$$(6)=(2,\ \sqrt{10})^2(3,\ 1+\sqrt{10})(3,\ 1-\sqrt{10}).$$

Durch direkte Ausrechnung zeigt sich auch:

$$(2,\ \sqrt{10})^2=(4,\ 2\sqrt{10},\ 10)=(2)$$

$$(3,\ 1+\sqrt{10})(3,\ 1-\sqrt{10})=(9,\ 3+3\sqrt{10},\ 3-3\sqrt{10},\ 6)=(3).$$

Auf ähnliche Weise findet man:

$$(5) = (5, \sqrt{10})(5, \sqrt{10})$$
$$(13) = (13, 6 + \sqrt{10})(13, 6 - \sqrt{10}).$$

3. Beispiel: $k(\sqrt{-15})$.

Für diesen Körper ist:

$$m = -15 \equiv 1, (4),$$

also sind die ganzen Zahlen:

$$a + b\,\frac{1+\sqrt{-15}}{2} = a + b\omega.$$

Man verifiziert leicht die folgenden Zerlegungen:

$$(2) = (2, \omega)(2, \omega')$$
$$(3) = (3, \sqrt{-15})^2 = (3, -1 + 2\omega)^2$$
$$(5) = (5, \sqrt{-15})^2 = (5, -1 + 2\omega)^2$$
$$(17) = (17, 5 + \omega)(17, 5 + \omega')$$

u. a. Unter diesen sind $(3, \sqrt{-15})$ und $(5, \sqrt{-15})$ offenbar noch nicht in der kanonischen Form. Um diese aufzustellen, hat man $\sqrt{-15}$ durch die Basis auszudrücken und erhält dann leicht:

$$(3, \sqrt{-15}) = (3, -1 + 2\omega, 3\omega - (-1 + 2\omega)) = (3, 1 + \omega),$$
$$(5, \sqrt{-15}) = (5, -1 + 2\omega, 5\omega - 2(-1 + 2\omega)) = (5, 2 + \omega).$$

10. Körper mit lauter Hauptidealen.

Für diejenigen Körper, für welche das Euklidische Teilerverfahren gilt, kann man folgenden Satz aussprechen:

Satz. *Gilt für einen quadratischen Körper unbeschränkt das Euklidische Teilerverfahren, so gilt auch zugleich der Satz von der eindeutigen Zerlegbarkeit aller Zahlen, und es sind alle Ideale des Körpers Hauptideale.*

Beweis. Der Körper $k(\sqrt{m})$ erfülle die im Satz gestellte Bedingung, und es sei

$$\mathfrak{a} = (\alpha, \beta, \gamma, \ldots)$$

irgend ein Ideal dieses Körpers. Dann ist die Behauptung des Satzes, daß das Ideal $\mathfrak{a}$ auch den größten gemeinsamen Teiler aller Zahlen $\alpha, \beta, \gamma \ldots$ enthält, welcher durch wiederholte Anwendung des Euklidischen Teilerverfahrens sich ergibt. Wir beweisen zunächst, daß, wenn α durch β nicht teilbar ist, aber ϱ_n den größten gemeinsamen

Teiler von α und β bedeutet, auch ϱ_n dem Ideal angehört. Dazu setzen wir das Teilerverfahren in der Form an:

$$\begin{aligned}
&\alpha - \varkappa\beta - \varrho_0 &&= 0\\
&\qquad\beta - \varkappa_1\varrho_0 - \varrho_1 &&= 0\\
&\qquad\qquad\varrho_0 - \varkappa_2\varrho_1 - \varrho_2 &&= 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&-\varrho_n \qquad\qquad + \varrho_{n-2} - \varkappa_n\varrho_{n-1} &&= 0.
\end{aligned}$$

Diese $n+1$ Gleichungen kann man auffassen als ein simultanes System für die n Unbekannten $\varrho_0, \varrho_1, \ldots \varrho_{n-1}$, woraus als Eliminationsgleichung sofort folgt:

$$0 = \begin{vmatrix}
\alpha - \varkappa\beta & -1 & 0 & 0 & . & 0\\
\beta & -\varkappa_1 & -1 & 0 & . & 0\\
0 & 1 & -\varkappa_2 & -1 & . & 0\\
. & . & . & . & . & .\\
0 & . & 0 & 1 & -\varkappa_{n-1} & -1\\
-\varrho_n & & & & 1 & -\varkappa_n
\end{vmatrix}.$$

Die $\varkappa$ sind sämtlich ganze Zahlen des Körpers, also folgt durch Ausrechnung der Determinante:

$$\varrho_n = \lambda_1\alpha + \lambda_2\beta.$$

Weil hierin λ_1, λ_2 wieder ganze Zahlen des Körpers sind, so gehört ϱ_n dem Ideal an. Durch Wiederholung dieses Schlußverfahrens folgt somit, daß auch A, der größte gemeinsame Teiler aller Zahlen α, β, $\gamma, \ldots,$ dem Ideal angehört, also ist

$$\mathfrak{a} = (\mathsf{A}).$$

Man kann den angeführten Satz auch umkehren und sagen, wenn in einem Körper alle Ideale Hauptideale sind, so gilt in diesem Körper für alle Zahlen der Satz von der eindeutigen Zerlegbarkeit.

11. Kongruenzen nach Idealen.

Wir schreiben:

$$\alpha \equiv 0, \ (\mathfrak{a}),$$

(gesprochen α kongruent Null Modulo $\mathfrak{a}$), wenn α und $\mathfrak{a}$ demselben Zahlkörper angehören und α in dem Ideal $\mathfrak{a}$ vorkommt, ferner sei für zwei ganze Zahlen des Körpers:

$$\alpha \equiv \beta, \ (\mathfrak{a})$$

(gesprochen α kongruent β modulo $\mathfrak{a}$), wenn die Differenz $\alpha - \beta$ im Ideal $\mathfrak{a}$ vorkommt. Gehört aber α, resp. $\alpha - \beta$ dem Ideal $\mathfrak{a}$ nicht an, so schreiben wir:

$$\alpha \not\equiv 0,\ (\mathfrak{a}), \quad \text{resp.} \quad \alpha \not\equiv \beta,\ (\mathfrak{a}),$$

(gespr. α inkongruent 0, resp. β modulo $\mathfrak{a}$).

Anmerkung. Diese Definition der Kongruenz ist zunächst rein formal eingeführt. Man sieht aber sofort, daß die Definition mit derjenigen für *Kongruenzen nach Zahlen* übereinstimmt, wenn $\mathfrak{a}$ ein Hauptideal, also $\mathfrak{a} = (\bar{\alpha})$ ist. Später kann noch bewiesen werden, daß auch für den Fall, wo $\mathfrak{a}$ ein beliebiges Ideal ist, die Definition im wesentlichen identisch ist mit der früher gegebenen Definition der Kongruenz: Die Kongruenz $\alpha \equiv 0, (\mathfrak{a})$ sagt eben aus, daß das Ideal (α) durch $\mathfrak{a}$ teilbar ist.

Erinnern wir uns der Definition der Ideale und des Produkts $\mathfrak{a}$ zweier Ideale $\mathfrak{b}$ und $\mathfrak{c}$, so kann man offenbar folgende Ausdrucksweise gebrauchen:

Ist ein Ideal $\mathfrak{a}$ teilbar durch ein Ideal $\mathfrak{b}$, so gelten für die sämtlichen Zahlen $\alpha, \beta, \gamma \ldots$ aus $\mathfrak{a}$ die Kongruenzen:

$$\alpha \equiv 0,\ (\mathfrak{b}), \quad \beta \equiv 0,\ (\mathfrak{b}), \quad \gamma \equiv 0,\ (\mathfrak{b}) \quad \text{usw.}$$

Auch die Umkehrung dieses Satzes wird später bewiesen.

Man kann nun, falls irgend ein Ideal $\mathfrak{a}$ gegeben ist, die sämtlichen ganzen Zahlen des Körpers in Klassen einteilen, indem man alle Zahlen, welche einer bestimmten Zahl mod. $\mathfrak{a}$ kongruent sind, einer Klasse zurechnet. Es sind dann irgend zwei Zahlen einer Klasse nach dem Modul $\mathfrak{a}$ kongruent, und daraus folgt, daß eine beliebige Zahl einer Klasse immer nur wieder dieselbe Klasse bestimmt, oder jede ganze Zahl gehört nur einer einzigen Klasse an.

Die Anzahl dieser Zahlklassen ist offenbar so zu berechnen, daß man nach dem vollen System von Zahlen fragt, von welchen nie zwei einander nach dem Modul $\mathfrak{a}$ kongruent sind, oder welche, anders ausgedrückt, ein vollständiges Restsystem nach dem Ideal $\mathfrak{a}$ bilden.

Satz. *Die Anzahl aller nach einem Ideal*

$$\mathfrak{a} = (i,\ i_1 + i_2\omega)$$

inkongruenten ganzen Zahlen ist:

$$n(\mathfrak{a}) = |\, i i_2 \,|.$$

Beweis. Die Inkongruenz:

$$a + b\omega \not\equiv 0,\ (i,\ i_1 + i_2\omega)$$

besteht offenbar für alle Kombinationen der Zahlen

$$\left.\begin{array}{l} a = 0,\ 1,\ 2,\ \ldots\ i - 1 \\ b = 0,\ 1,\ 2,\ \ldots\ i_2 - 1, \end{array}\right\} \qquad (C)$$

(wo wir i und i_2 positiv voraussetzen, was immer allgemein geschehen kann), weil jede Zahl des Ideals von der Form

$$l_1 i + l_2(i_1 + i_2\omega)$$

mit den ganzzahligen rationalen Koeffizienten l_1 und l_2 sein muß. Die Kombinationen (C) bilden ein System von $i i_2$ Zahlen, von denen 1.) keine zwei einander kongruent sein können nach dem Modul $\mathfrak{a}$. Die Differenz irgend zweier Zahlen des Systems

$$a_k + b_k\omega - (a_{k'} + b_{k'}\omega)$$

ist nicht im Ideal enthalten. Dagegen ist 2.) irgend eine Zahl des Körpers *einer* und nur einer Zahl dieses Systems kongruent. In der Tat, da die $a = 0, \ldots i - 1$ und $b = 0, \ldots i_2 - 1$ je ein vollständiges Restsystem nach i, bezw. i_2 bilden, so kann man für eine gegebene ganze Zahl des Körpers $A + B\omega$ die Zahl $a + b\omega$ aus dem System so auswählen, daß die Gleichung:

$$A + B\omega - (a + b\omega) = l_1 i + l_2(i_1 + i_2\omega)$$

durch zwei ganze rationale Zahlen l_2 und l_1 befriedigt wird, für je *ein* bestimmtes a und b. Denn es sind nun a, b z. B. so zu wählen, daß nach einander die Kongruenzen gelten:

$$b \equiv B, (i_2); \quad B - b = l_2 i_2$$
$$a \equiv A - l_2 i_1, (i).$$

Die Zahl $n(\mathfrak{a})$ hat also nach dem eben bewiesenen Satz eine besondere Bedeutung. Man nennt sie die *Norm des Ideals* $\mathfrak{a}$. Es ist wichtig für die Definition der Norm, daß dieselbe von der speziellen Wahl der Basis unabhängig ist. Sei nämlich ι_1^*, ι_2^* eine beliebige Basis des Ideals $\mathfrak{a}$, und sei etwa $\iota_1^* = a_1 + b_1\omega$ und $\iota_2^* = a_2 + b_2\omega$, dann gibt es vier ganze rationale Zahlen r, s, t, u mit der Bedingung $ru - ts = \pm 1$, so daß $\iota_1^* = ri + s(i_1 + i_2\omega)$, $\iota_2^* = ti + u(i_1 + i_1\omega)$ ist, und es folgt aus dem Multiplikationssatz für Determinanten:

$$n(\mathfrak{a}) = |(a_1 b_2 - a_2 b_1)| = i i_2.$$

Für das Produkt zweier Ideale besteht der Satz:

Die Norm des Produkts zweier Ideale ist gleich dem Produkt der Normen derselben.

Der Beweis dieser Behauptung auf Grund der bisherigen Definition wird später bei den Idealen eines kubischen Körpers auszuführen sein. Umsomehr kann daher an dieser Stelle der Satz als Folge einer andern Definition der Norm abgeleitet werden.

12. Die Norm eines Ideals als Idealprodukt.

Ersetzt man in einem Ideal $\mathfrak{a}$ alle Zahlen durch ihre Konjugierten, also $\alpha, \beta, \gamma, \ldots$ durch $\alpha', \beta', \gamma', \ldots$ oder ersetzt man in allen Zahlen ω durch ω', so erhält man wieder ein Ideal $\mathfrak{a}'$, und $\mathfrak{a}'$ heißt das zu $\mathfrak{a}$ *konjugierte* Ideal.

Ein Ideal und sein konjugiertes Ideal mögen von nun ab mit dem gleichen Buchstaben geschrieben und durch den Akzent unterschieden werden, indem man dieselben mit $\mathfrak{a}$ resp. $\mathfrak{a}'$ bezeichnet. Will man andeuten, daß $\mathfrak{a}'$ aus $\mathfrak{a}$ dadurch entstanden ist, daß in jeder ganzen Zahl von $\mathfrak{a}$ die Substitution $s(\sqrt{m} : -\sqrt{m})$ vorgenommen ist, so schreibt man wohl auch $s(\mathfrak{a})$ statt $\mathfrak{a}'$.

Ein Ideal $\mathfrak{a}$ heißt ein *ambiges* Ideal, wenn dasselbe mit seinem konjugierten Ideal übereinstimmt, wenn also $\mathfrak{a} = \mathfrak{a}'$ ist, und wenn dasselbe durch keine ganze rationale Zahl (kein rationales Hauptideal) außer ± 1 teilbar ist.

Satz. *Das Produkt aus einem Ideal und seinem konjugierten Ideal ist ein rationales Hauptideal, und zwar ist:*

$$\mathfrak{a} \cdot \mathfrak{a}' = (n(\mathfrak{a})).$$

Beweis.[1]) Es sei:

$$\mathfrak{a} = (i, i_1 + i_2\omega), \quad \mathfrak{a}' = (i, i_1 + i_2\omega'),$$

dann ist bewiesen worden, daß i und i_1 Vielfache von i_2 sind, man kann also setzen:

$$i = a i_2, \quad i_1 = a_1 i_2,$$

und danach ist:

$$\mathfrak{a} = (a i_2, a_1 i_2 + i_2\omega) = (i_2)(a, a_1 + \omega),$$

und analog:

$$\mathfrak{a}' = (i_2)(a, a_1 + \omega');$$

ferner gilt für a und a_1 die Relation:

$$(a_1 + \omega)(a_1 + \omega') \equiv 0, \ (a),$$

weil a der größte gemeinsame Faktor aller reellen Zahlen in den Idealen $(a, a_1 + \omega)$ und $(a, a_1 + \omega')$ ist. Nun ergibt die Multiplikation der beiden Ideale:

$$\begin{aligned}\mathfrak{a} \cdot \mathfrak{a}' &= (i_2)(a, a_1 + \omega) \cdot (i_2)(a, a_1 + \omega') \\ &= (i_2^2)(a^2, aa_1 + a\omega, aa_1 + a\omega', (a_1 + \omega)(a_1 + \omega'))\end{aligned}$$

und es bleibt nur noch nachzuweisen, daß der zweite Faktor dieses

1) Dieser Beweis ist von Herrn Hilbert in seinen Vorlesungen 1897/98 entwickelt worden.

Produkts ein rationales Hauptideal gleich (a) ist. Wir unterscheiden dazu drei Fälle der Körper $k(\sqrt{m})$.

1. Fall. $m \equiv 3, (4), \omega = \sqrt{m}, \omega' = -\sqrt{m}$.

Alsdann gelten die Gleichungen:

$$\begin{aligned}&(a^2, aa_1 + a\omega, aa_1 + a\omega', (a_1 + \omega)(a_1 + \omega'))\\ &= (a^2, aa_1 + a\sqrt{m}, aa_1 - a\sqrt{m}, a_1^2 - m)\\ &= (a^2, 2aa_1, 2a\sqrt{m}, 2am, a_1^2 - m)\\ &= (a)\left(a, 2m, \frac{a_1^2 - m}{a}, 2a_1, 2\sqrt{m}\right).\end{aligned}$$

Nun können die Zahlen a, $2m$ und $\frac{a_1^2 - m}{a}$ *keinen gemeinsamen Faktor mehr besitzen.* Angenommen zunächst, $q > 2$ sei in a und m enthalten, dann ist

$$a_1^2 - m \equiv 0, (q) \quad (\text{denn } a_1^2 - m \equiv 0, (a))$$

und da

$$m \equiv 0, (q),$$

so folgt

$$a_1 \equiv 0, (q).$$

Weil nun aber m keine quadratischen Faktoren enthält, a_1^2 aber durch q^2 teilbar ist, so ersieht man aus der Umformung

$$a_1^2 - m = q\left(\frac{a_1^2}{q} - \frac{m}{q}\right),$$

daß $a_1^2 - m$ durch keine höhere Potenz von q als q^1 teilbar sein kann, also ist:

$$\frac{a_1^2 - m}{a} \not\equiv 0, (q).$$

Geht ferner $q = 2$ in a auf, so ist 2 Faktor von a und $2m$; wegen $a_1^2 - m \equiv 0, (a)$ muß dann a_1 ungerade sein, also wird

$$a_1^2 - m \equiv -2, (4),$$

somit ist

$$\frac{a_1^2 - m}{a}$$

ungerade und prim zu 2.

Folglich haben in diesem ersten Fall die drei Zahlen a, $2m$, $\frac{a_1^2 - m}{a}$ keinen gemeinsamen Teiler und man kann daher drei andere ganze rationale Zahlen l_1, l_2, l_3 angeben, derart, daß $l_1 a + l_2 2m + l_3 \frac{a_1 - m}{a} = 1$ wird. Es ergibt sich also:

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a),$$

und schließlich

$$\mathfrak{a} \cdot \mathfrak{a}' = (i_2^2)(a) = (a i_2^2) = (i i_2),$$

oder wie die Behauptung verlangt:

$$\mathfrak{a}\mathfrak{a}' = (n(\mathfrak{a})).$$

2. **Fall.** $m \equiv 2, (4), \ \omega = \sqrt{m}, \ \omega' = -\sqrt{m}.$

Dann ist ähnlich wie im ersten Fall:

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a)\left(a, 2m, \frac{a_1^2 - m}{a}, 2a_1, 2\sqrt{m}\right),$$

und es enthalten die drei Zahlen a, $2m$ und $\frac{a_1^2 - m}{a}$ jedenfalls wieder keinen gemeinsamen Faktor $q > 2$. Sie können aber auch nicht den Faktor $q = 2$ gleichzeitig enthalten. In der Tat, wegen

$$a_1^2 - m \equiv 0, \ (a)$$

muß nämlich alsdann a_1 gerade sein, und es wird

$$a_1^2 - m \equiv -2, \ (4),$$

d. h. $a_1^2 - m$ ist nur durch 2 teilbar, oder es ist

$$\frac{a_1^2 - m}{a} \not\equiv 0, \ (2).$$

Aus den drei Zahlen a, $2m$, $\frac{a_1^2 - m}{a}$ kann man folglich wiederum die 1 zusammensetzen, d. h. es ist wieder, wie im ersten Fall:

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a)$$

und

$$\mathfrak{a}\mathfrak{a}' = (a i_2^2) = (n(\mathfrak{a})).$$

3. **Fall.** $m \equiv 1, (4), \ \omega = \frac{1 + \sqrt{m}}{2}, \ \omega' = \frac{1 - \sqrt{m}}{2}.$

Dann ist:

$$(a, a_1 + \omega)(a, a_1 + \omega') = \left(a^2, 2aa_1 + a, a\sqrt{m}, \left(a_1 + \frac{1}{2}\right)^2 - \frac{m}{4}\right)$$

$$= (a)\left(a, m, \frac{\left(a_1 + \frac{1}{2}\right)^2 - \frac{m}{4}}{a}, 2a_1 + 1, \sqrt{m}\right),$$

und es enthalten die vier Zahlen a, m, $\frac{\left(a_1 + \frac{1}{2}\right)^2 - \frac{m}{4}}{a}$, $2a_1 + 1$ jedenfalls nicht den Faktor 2, weil die letzte sicher ungerade ist. Enthalten a und m einen Faktor $q > 2$, so ist doch sicher $\frac{\left(a_1 + \frac{1}{2}\right)^2 - \frac{m}{4}}{a}$ prim zu q, weil $\left(a_1 + \frac{1}{2}\right)^2$ diesen Faktor quadratisch, $\frac{m}{4}$ ihn aber nur ein-

fach enthält. Man kann folglich aus den vier Zahlen wieder die 1 zusammensetzen und hat:

$$(a,\ a_1+\omega)\,(a,\ a_1+\omega')=(a),$$

also

$$\mathfrak{a}\cdot\mathfrak{a}'=(i_2^2)\,(a)=(a i_2^2)=(i i_2),$$

oder wieder wie in den beiden ersten Fällen:

$$\mathfrak{a}\cdot\mathfrak{a}'=(n(\mathfrak{a})).$$

Die Zahl $n(\mathfrak{a})=i i_2$ gehört selbst auch unter die Zahlen von $\mathfrak{a}$, wie auch von $\mathfrak{a}'$. Wenn das Ideal $\mathfrak{a}$ nicht in der kanonischen Darstellung, sondern durch die Basis $\iota_1^*=a_1+b_1\omega$, $\iota_2^*=a_2+b_2\omega$ gegeben ist, so ist ebenfalls, wie in der vorhergehenden Nummer gezeigt wurde: $\mathfrak{a}\mathfrak{a}'=(n(\mathfrak{a}))=(a_1 b_2-a_2 b_1)$.

Hat man jetzt ein Produkt aus lauter Idealen:

$$\mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}\ldots\mathfrak{k},$$

so folgt aus dem eben ausgeführten Satz für die Norm dieses Produktes:

$$n(\mathfrak{a}\cdot\mathfrak{b}\cdot\mathfrak{c}\ldots\mathfrak{k})=n(\mathfrak{a})\cdot n(\mathfrak{b})\cdot n(\mathfrak{c})\ldots n(\mathfrak{k}),$$

denn es gelten die Idealgleichungen:

$$(n(\mathfrak{a}\cdot\mathfrak{b}\cdot\mathfrak{c}\ldots\mathfrak{k}))=\mathfrak{a}\cdot\mathfrak{b}\cdot\mathfrak{c}\ldots\mathfrak{k}\cdot\mathfrak{a}'\cdot\mathfrak{b}'\cdot\mathfrak{c}'\ldots\mathfrak{k}'=(n(\mathfrak{a}))\,(n(\mathfrak{b}))\,(n(\mathfrak{c}))\ldots(n(\mathfrak{k})).$$

Eine wichtige Folgerung, welche aus dem allgemeinen Satz über die Norm eines beliebigen Ideals zu ziehen ist, bezieht sich auf die Anzahl der Zahlen eines vollständigen Restsystems nach einer ganzen Zahl des Körpers.

Satz. *Bedeutet α eine beliebige ganze Zahl des Körpers $k(\sqrt{m})$, so enthält das vollständige Restsystem nach dieser Zahl $|n(\alpha)|$ Zahlen.*

Beweis. Die gesuchte Anzahl ist gerade so groß, wie die Anzahl der Zahlen eines vollständigen Restsystems nach dem Hauptideal $(\alpha)=\mathfrak{a}$. Als Basis des Ideals $\mathfrak{a}$ kann man aber wählen $\iota_1^*=\alpha$ und $\iota_2^*=\alpha\omega$. Setzt man $\alpha=a+b\omega$, so hat man

1. für den Fall $m\equiv 1,\ (4)$:

$$\iota_1^*=a+b\omega$$

$$\iota_2^*=b\,\frac{m-1}{4}+(a+b)\omega,$$

und daher ist:

$$n(\mathfrak{a})=\left|\,a^2+ab-\frac{m-1}{4}b^2\,\right|=|\,n(\alpha)\,|,$$

2. für den Fall $m\not\equiv 1,\ (4)$:

$$\iota_1^*=a+b\omega$$

$$\iota_2^*=bm+a\omega,$$

also wieder:

$$n(\mathfrak{a}) = |a^2 - b^2 m| = |n(\alpha)|.$$

Beispiele. I. Es sei $\alpha = x + y\sqrt{-1}$ eine ganze Zahl des Körpers $k(\sqrt{-1})$, so ist also $n(\alpha) = x^2 + y^2$. Da in diesem Körper der Satz von der eindeutigen Zerlegbarkeit der ganzen Zahlen gilt, so sind alle Ideale Hauptideale. Wenn nun $\pi = x + y\sqrt{-1}$ eine nicht rationale Primzahl des Körpers ist, so muß $n(\pi) = \pi \cdot \pi'$ eine rationale Primzahl p sein, was man daraus folgert, daß es eine rationale Zahl ist. Das Restsystem nach einer solchen Primzahl π enthält daher p Zahlen des Körpers. Ist dagegen eine rationale Primzahl q auch im Körper $k(\sqrt{-1})$ unzerlegbar, so ist $n(q) = q^2$. Z. B. ist

$$5 = (2 + \sqrt{-1})(2 - \sqrt{-1}),$$

und es stellen die fünf Zahlen $0, 1, 2, \sqrt{-1}, 1 + \sqrt{-1}$ ein vollständiges Restsystem nach $\alpha = 2 + \sqrt{-1}$ dar.[1]) Jede andere Zahl des Körpers ist einer dieser fünf Zahlen nach α kongruent, z. B.:

$$-\sqrt{-1} \equiv 2, (\alpha), \quad -2 \equiv \sqrt{-1}, (\alpha), \quad -1 \equiv 1 + \sqrt{-1}, (\alpha)$$
$$3 \equiv \sqrt{-1}, (\alpha), \quad 4 \equiv 1 + \sqrt{-1}, (\alpha) \quad \text{usw.}$$

Ebenso stellen die 9 Zahlen $0, \sqrt{-1}, 2\sqrt{-1}, 1, 1 + \sqrt{-1}, 1 + 2\sqrt{-1}, 2, 2 + \sqrt{-1}, 2 + 2\sqrt{-1}$ ein vollständiges Restsystem[2]) nach 3 dar, weil 3 im Körper $k(\sqrt{-1})$ nicht zerlegbar ist.

II. Im Körper $k(\sqrt{-5})$ ist z. B. $(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$ und es bilden die drei Zahlen 0, 1, 2 ein vollständiges Restsystem nach $\mathfrak{p} = (3, 1 + \sqrt{-5})$ oder $\mathfrak{p}' = (3, 1 - \sqrt{-5})$; ferner ist $\mathfrak{p} = (11)$ ein Primideal zweiten Grades des Körpers, und es stellen die 121 Zahlen: $a + b\sqrt{-5}$ für sämtliche Kombinationen $a = 0, 1, \ldots 10$, $b = 0, 1, 2, \ldots 10$ ein vollständiges Restsystem nach $\mathfrak{p} = (11, 11\sqrt{-5})$ vor.

Für spätere Anwendung zum Beweise der eindeutigen Zerlegbarkeit der Ideale in Primfaktoren ist folgender Satz sehr wichtig:

Satz. *Ein Ideal ist nur durch eine endliche Anzahl Ideale teilbar.*

Beweis. Es sei

$$\mathfrak{j} = \mathfrak{a}\,\mathfrak{b}\,\mathfrak{c} \ldots,$$

1) Statt dieser Zahlen, deren Aufstellung ohne weiteres klar ist, könnte man auch das System der „absolut kleinsten Reste" nehmen (siehe S. 29). In dem Beispiele wären dies die Zahlen: $0, \pm 1, \pm\sqrt{-1}$.

2) Das System der absolut kleinsten Reste wäre: $0, \pm 1, \pm\sqrt{-1}, \pm 1 \pm \sqrt{-1}$.

so ist:

$$(n(\mathfrak{j})) = (n(\mathfrak{a}))\,(n(\mathfrak{b}))\,(n(\mathfrak{c}))\,\ldots.$$

Nun ist aber $n(\mathfrak{j})$ eine ganze rationale Zahl und kann nur durch eine endliche Anzahl von rationalen ganzen Zahlen > 1 teilbar sein, also kann die Zahl der Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ... nur endlich sein, vorausgesetzt natürlich, daß von Einheitsidealen abgesehen wird.

Durch Kombination der drei vorhergehenden Sätze erhält man schließlich das folgende Resultat:

Satz. *Es gibt nur eine endliche Anzahl Ideale, deren Norm kleiner ist als eine endliche rationale Zahl.*

Diesen letzten Satz kann man in etwas anderer Form auch so aussprechen:

Es gibt nur eine endliche Anzahl verschiedener Ideale, welche eine gegebene endliche Zahl α gleichzeitig enthalten.

Geht ein Ideal in einer rationalen Primzahl p auf, so ist jedenfalls p eine Zahl des Ideals, und es muß in der kanonischen Darstellung

$$(i,\; i_1 + i_2\,\omega)$$

i direkt gleich p sein, da man ja aus zwei Zahlen p und $i < p$, weil sie zueinander prim sind, die 1 zusammensetzen könnte, und andererseits $i = 1$ einem Einheitsideal entspräche. Für die Zahl i_2, die ein Teiler von $i = p$ sein muß, bleiben noch zwei Möglichkeiten: entweder es ist $i_2 = 1$ und $i_1 < p$ sonst noch unbekannt, oder es ist $i_2 = p$, und i_1, welches dann auch ein Vielfaches von p ist, kann 0 gesetzt werden. Den beiden Möglichkeiten

$$(p,\; i_1 + \omega) \quad \text{und} \quad (p,\; p\,\omega)$$

entsprechen die Normen p resp. p^2.

Satz. *Die Norm eines Ideals, das in einer rationalen Primzahl p aufgeht, ist entweder p oder p^2.*

Im ersten Fall soll das Ideal ein *Ideal ersten Grades*, im zweiten Fall ein *Ideal zweiten Grades* genannt werden.

Beispiele. Wir nehmen zuerst die schon behandelten Körper wieder vor und berechnen die Normen der Ideale entsprechend den beiden Definitionen.

1. Beispiel: $k(\sqrt{-5})$.

1. $\mathfrak{j} = (2,\; 1 + \sqrt{-5})$, $\mathfrak{j}' = (2,\; 1 - \sqrt{-5})$,

dann ist nach dem allgemeinen Satz $n(\mathfrak{j}) = 2$ und:

$$\mathfrak{j}\mathfrak{j}' = (4,\; 2 + 2\sqrt{-5},\; 2 - 2\sqrt{-5},\; 6,\; 2) = (2).$$

2. $\mathfrak{j} = (3,\ 1 + \sqrt{-5})$, $\mathfrak{j}' = (3,\ 1 - \sqrt{-5})$,
dann ist:

$n(\mathfrak{j}) = 3$, und $\mathfrak{j}\mathfrak{j}' = (9,\ 3 + 3\sqrt{-5},\ 3 - 3\sqrt{-5},\ 6,\ 3) = (3)$.

3. $\mathfrak{j} = (4 + \sqrt{-5},\ 1 + 2\sqrt{-5})$, $\mathfrak{j}' = (4 - \sqrt{-5},\ 1 - 2\sqrt{-5})$,

$n(\mathfrak{j}) = 7$, und $\mathfrak{j}\mathfrak{j}' = (21, 14 + 7\sqrt{-5}, 14 - 7\sqrt{-5}, 28, 7) = (7)$.

4. $\mathfrak{j} = (4 - \sqrt{-5},\ 1 + 2\sqrt{-5})$, $\mathfrak{j}' = (4 + \sqrt{-5},\ 1 - 2\sqrt{-5})$,
es ist

$$\mathfrak{j}\mathfrak{j}' = (21, -6 + 9\sqrt{-5}, -6 - 9\sqrt{-5}, -12, 3) = (3),$$

also $n(\mathfrak{j}) = 3$, und in der Tat sieht man leicht, daß das vorliegende Beispiel mit demjenigen von 2.) identisch ist.

5. $\mathfrak{j} = (21,\ 10 + \sqrt{-5})$, $\mathfrak{j}' = (21,\ 10 - \sqrt{-5})$,

$n(\mathfrak{j}) = 21$ und $\mathfrak{j}\mathfrak{j}' = (441, 210 + 21\sqrt{-5}, 210 - 21\sqrt{-5}, 105) = (21)$.

2. Beispiel: $k(\sqrt{-15})$.

1. $\mathfrak{j} = (2,\ \omega) = \left(2,\ \frac{1 + \sqrt{-15}}{2}\right)$, $\mathfrak{j}' = \left(2,\ \frac{1 - \sqrt{-15}}{2}\right)$,

$n(\mathfrak{j}) = 2$, und $\mathfrak{j}\mathfrak{j}' = (4, 1 + \sqrt{-15}, 1 - \sqrt{-15}, 2) = (4, 2\omega, 2\omega', 2) = (2)$.

2. $\mathfrak{j} = (3, \sqrt{-15})$, $\mathfrak{j}' = (3,\ -\sqrt{-15}) = (3,\ 1 + \omega)$,

$n(\mathfrak{j}) = 3$, und $\mathfrak{j}\mathfrak{j}' = (9,\ 3\sqrt{-15},\ 15,\ 3) = (3)$.

3. $\mathfrak{j} = (17,\ 5 + \omega)$, $\mathfrak{j}' = (17,\ 5 + \omega')$,

$n(\mathfrak{j}) = 17$, und $\mathfrak{j}\mathfrak{j}' = (289, 85 + 17\omega, 85 + 17\omega', 34) = (17)$.

4. $\mathfrak{j} = (93,\ 13 + \omega)$, $n(\mathfrak{j}) = 93$,
denn es ist

$$\mathfrak{j}\mathfrak{j}' = (93^2,\ 13 \cdot 93 + 93\omega,\ 13 \cdot 93 + 93\omega',\ 186,\ 93) = (93).$$

Ich überlasse es dem Leser, zur Übung noch die vollständigen Restsysteme für die vorstehenden Ideale aufzustellen.

13. Eindeutige Zerlegbarkeit der Ideale.

Definiert man *Primideale* als solche Ideale, welche verschieden sind von Einheitsidealen und welche nur durch sich selbst und durch Einheitsideale geteilt werden können, so ist man jetzt imstande, den Fundamentalsatz der Idealtheorie zu beweisen, d. h. den Satz, daß jedes Ideal auf eine und nur eine Weise in Primideale zerlegbar ist.

Zum Beweise des Fundamentalsatzes müssen noch eine Reihe von Hilfssätzen vorausgeschickt werden:

Satz. *Sind* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *irgend drei von Null verschiedene Ideale, und gilt:*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c},$$

so ist $\mathfrak{b} = \mathfrak{c}$.

Beweis. Man multipliziere die Idealgleichung mit $\mathfrak{a}'$, dann ist:

$$\mathfrak{a}'\mathfrak{a}\,\mathfrak{b} = \mathfrak{a}'\mathfrak{a}\,\mathfrak{c},$$

$$(n(\mathfrak{a}))\mathfrak{b} = (n(\mathfrak{a}))\,\mathfrak{c},$$

und da man den Zahlenfaktor $n(\mathfrak{a})$ heben kann, so folgt:

$$\mathfrak{b} = \mathfrak{c}.$$

Satz. *Sind alle Zahlen eines Ideals* $\mathfrak{a}$ *kongruent Null nach einem andern Ideal* $\mathfrak{b}$, *so ist* $\mathfrak{a}$ *teilbar durch* $\mathfrak{b}$.

Beweis. Die Ideale seien $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots)$ und $\mathfrak{b} = (\beta_1, \beta_2, \ldots)$, dann ist also die Voraussetzung:

$$\alpha_1 \equiv 0,\ (\mathfrak{b})$$
$$\alpha_2 \equiv 0,\ (\mathfrak{b})$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

Zum Beweise des Satzes multipliziert man $\mathfrak{a}$ sowohl als $\mathfrak{b}$ mit $\mathfrak{b}'$, alsdann ist:

$$\mathfrak{b}\mathfrak{b}' = (n(\mathfrak{b})),$$

und nun läßt sich zunächst zeigen, daß $\mathfrak{a}\mathfrak{b}'$ durch $\mathfrak{b}\mathfrak{b}'$ teilbar ist. Wirklich gilt für *alle* Zahlen aus $\mathfrak{a}\mathfrak{b}'$ die Kongruenz:

$$\alpha_1\beta_1' \equiv 0, \quad \alpha_1\beta_2' \equiv 0, \ \ldots\ (\mathfrak{b}\mathfrak{b}')$$
$$\alpha_2\beta_1' \equiv 0, \quad \alpha_2\beta_2' \equiv 0, \ \ldots\ (\mathfrak{b}\mathfrak{b}'), \ \text{usw.};$$

weil aber $\mathfrak{b}\mathfrak{b}' = (n(\mathfrak{b}))$ ein rationales Hauptideal darstellt, so kann man setzen:

$$\alpha_1\beta_1' = n(\mathfrak{b}) \cdot \gamma_{11}, \quad \alpha_1\beta_2' = n(\mathfrak{b})\,\gamma_{12}\ \ldots$$
$$\alpha_2\beta_1' = n(\mathfrak{b}) \cdot \gamma_{21}, \quad \alpha_2\beta_2' = n(\mathfrak{b})\,\gamma_{22}\ \ldots, \quad \text{usw.},$$

wo jetzt $\gamma_{11}, \gamma_{12} \ldots$ ganze Zahlen des Körpers sind, und man sieht unmittelbar, daß die Gleichung besteht:

$$\mathfrak{a} \cdot \mathfrak{b}' = (n(\mathfrak{b}))\,(\gamma_{11}, \gamma_{12}, \ldots).$$

Hier muß $(\gamma_{11}, \gamma_{12}, \ldots) = \mathfrak{c}$ wieder ein Ideal sein, da es ja aus dem Ideal $\mathfrak{a}\mathfrak{b}'$ durch Abscheidung des gemeinsamen Faktors $n(\mathfrak{b})$ aller Zahlen des Ideals hervorging. Es ist somit:

$$\mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{b}'\mathfrak{c},$$

und mit Berücksichtigung des ersten Hilfssatzes:

$$\mathfrak{a} = \mathfrak{b}\mathfrak{c},$$

wie es der Satz verlangt.

Folgerung. *Der größte gemeinsame Teiler* $\mathfrak{t}$ *zweier Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *ist ein Ideal, welches alle Zahlen aus* $\mathfrak{a}$ *und* $\mathfrak{b}$ *zugleich enthält.*

Ist

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots), \quad \mathfrak{b} = (\beta_1, \beta_2, \ldots),$$

so ist

$$\mathfrak{t} = (\alpha_1, \alpha_2, \ldots \beta_1, \beta_2, \ldots).$$

In der Tat muß ja ein Ideal, das in $\mathfrak{a}$ und $\mathfrak{b}$ aufgeht, alle Zahlen von $\mathfrak{a}$ resp. von $\mathfrak{b}$ enthalten. Weil aber ein Ideal, das alle diese Zahlen und außerdem andere ganze Zahlen des Körpers enthält, die nicht durch lineare Kombination der α und β entstehen, seinerseits in $\mathfrak{t}$ aufgeht, so kann $\mathfrak{t}$ der größte gemeinsame Teiler von $\mathfrak{a}$ und $\mathfrak{b}$ heißen.

Satz. *Wenn ein Produkt aus zwei Idealen* $\mathfrak{a}$ *und* $\mathfrak{b}$ *teilbar ist durch ein Primideal* $\mathfrak{p}$ *und wenn dabei* $\mathfrak{b}$ *nicht teilbar ist durch* $\mathfrak{p}$, *so muß* $\mathfrak{a}$ *teilbar sein durch* $\mathfrak{p}$. Oder: *wenn das Produkt* $\mathfrak{a}\mathfrak{b}$ *durch ein Primideal* $\mathfrak{p}$ *teilbar ist, so muß mindestens einer der Faktoren* $\mathfrak{a}$, $\mathfrak{b}$ *durch* $\mathfrak{p}$ *teilbar sein.*

Beweis. Wir setzen $\mathfrak{a}$, $\mathfrak{b}$ an wie oben, ferner sei:

$$\mathfrak{p} = (\pi_1, \pi_2 \ldots).$$

Da nach Voraussetzung $\mathfrak{b}$ durch $\mathfrak{p}$ nicht teilbar ist, so gibt es außer den Einheitsidealen keine, welche in $\mathfrak{b}$ und $\mathfrak{p}$ zugleich aufgehen. Es ist also

$$\mathfrak{t} = (\beta_1, \beta_2, \ldots, \pi_1, \pi_2, \ldots)$$

ein Einheitsideal, und es läßt sich eine Zahl β aus $\mathfrak{b}$ und eine Zahl π aus $\mathfrak{p}$ so finden, daß $\beta + \pi = 1$ ist. Weil aber $\mathfrak{a}\mathfrak{b}$ teilbar sein soll durch $\mathfrak{p}$, so gelten die Kongruenzen:

$$\begin{array}{ll} \alpha_1\beta_1 \equiv 0, & \alpha_2\beta_1 \equiv 0, \ldots (\mathfrak{p}) \\ \alpha_1\beta_2 \equiv 0, & \alpha_2\beta_2 \equiv 0, \ldots (\mathfrak{p}) \\ \cdots & \cdots \\ \alpha_1\beta \equiv 0, & \alpha_2\beta \equiv 0, \ldots (\mathfrak{p}), \end{array}$$

und weil für die oben gewählte Zahl π: $\pi \equiv 0$, $(\mathfrak{p})$ ist, so ist offenbar auch:

$$\alpha_1(\beta + \pi) \equiv 0, \quad \alpha_2(\beta + \pi) \equiv 0, \ldots (\mathfrak{p}),$$

oder, weil $\beta + \pi = 1$ ist:

$$\alpha_1 \equiv 0, \quad \alpha_2 \equiv 0, \quad \alpha_3 \equiv 0, \ldots (\mathfrak{p}),$$

folglich ist $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar.

Auf Grund der bisherigen Hilfssätze ist nun der Fundamentalsatz leicht zu beweisen.

Fundamentalsatz. *Jedes Ideal läßt sich auf eine und nur auf eine einzige Weise in ein Produkt von Primidealen zerlegen.*

Beweis. Ist $\mathfrak{j}$ das gegebene Ideal, so suche man alle die Primideale, die in $\mathfrak{j}$ aufgehen:

$$\mathfrak{j} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_n.$$

Angenommen nun, es gäbe eine zweite Zerlegung:

$$\mathfrak{j} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \ldots \mathfrak{q}_m,$$

so wäre also

$$\mathfrak{q}_1 \cdot \mathfrak{q}_2 \ldots \mathfrak{q}_m = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_n.$$

Betrachten wir $\mathfrak{q}_1$, so muß dies in dem Produkt rechts aufgehen: es ist entweder ein Teiler von $\mathfrak{p}_1$, also dann gleich $\mathfrak{p}_1$, oder es ist prim zu $\mathfrak{p}_1$ und muß somit in dem Produkt $\mathfrak{p}_2 \ldots \mathfrak{p}_m$ aufgehen. Im letzteren Fall muß $\mathfrak{q}_1$ gleich $\mathfrak{p}_2$ sein, oder in dem Produkt $\mathfrak{p}_3 \ldots \mathfrak{p}_n$ aufgehen und alsdann würde man durch hinreichend oft wiederholte Anwendung desselben Schlusses folgern, daß $\mathfrak{q}_1$ mindestens einem der folgenden $\mathfrak{p}$ gleich ist. Man kann darum annehmen, daß

$$\mathfrak{p}_1 = \mathfrak{q}_1$$

ist, und schließt ebenso

$$\mathfrak{p}_2 = \mathfrak{q}_2$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot$$
$$\mathfrak{p}_n = \mathfrak{q}_m,$$

womit der Fundamentalsatz bewiesen ist.

Eine genaue Betrachtung des Beweises für den Fundamentalsatz zeigt, daß derselbe hauptsächlich auf der Tatsache beruht, daß $(n(\mathfrak{a})) = \mathfrak{a}\mathfrak{a}'$ ist, anders gefaßt, auf der Behauptung, daß zu einem gegebenen Ideal $\mathfrak{a}$ stets ein anderes $\mathfrak{a}'$ existiert, so daß $\mathfrak{a}\mathfrak{a}'$ ein rationales Hauptideal ist. Dieser Satz läßt sich durch den allgemeineren ersetzen: Zu jedem Ideal $\mathfrak{a}$ kann stets ein zweites Ideal $\mathfrak{a}_1$ so gefunden werden, daß das Produkt $\mathfrak{a} \cdot \mathfrak{a}_1$ ein Hauptideal wird. Diese Form des Satzes wird beim Beweise benützt, wenn ein allgemeiner algebraischer Zahlkörper zugrunde liegt. Die älteren Beweise von Dedekind (Suppl. XI) und Kronecker für den Fundamentalsatz der allgemeinen Idealtheorie waren sehr viel umständlicher, bis es auf Grund eines Satzes von Kronecker[1]) über die Teiler eines Systems ganzer Zahlen Herrn

1) Der Vollständigkeit wegen möge dieser Satz in seiner einfachsten Formulierung hier angeführt werden, indem der Inhalt desselben dem Leser nach dem Studium des 4. Abschnittes wohl verständlich sein wird:

Satz. Wenn die Koeffizienten $\alpha_0, \alpha_1 \ldots, \beta_0, \beta_1 \ldots$ der Funktionen einer Veränderlichen x:

Hurwitz[1]) zuerst gelang, die Theorie sehr zu vereinfachen. Unser Beweis soll einen Begriff der Entwicklungen dieses Mathematikers geben. Auf einen zweiten Beweis von Hurwitz wird sich an einer anderen Stelle eingehen lassen.

Einen einfachen Beweis ohne Benützung des Kroneckerschen Satzes, auf Grund des Begriffs des Galois'schen Körpers hat Herr Hilbert[2]) gegeben.

Zur praktischen Verwendung des Fundamentalsatzes fehlt noch eine Methode zur bequemen Entscheidung darüber, wann ein gegebenes Ideal Primideal ist, und wie die Faktoren eines Ideals, welches kein Primideal ist, gefunden werden können.

Die Lösung dieser Aufgaben liefert im wesentlichen schon die Tatsache, welche der folgende Satz ausspricht:

Satz. *Jedes Primideal* $\mathfrak{p}$ *des Körpers* $k(\sqrt{m})$ *ist stets Faktor einer rationalen Primzahl* p, *oder genauer gesagt eines Hauptideals* (p).

Bedeutet $\mathfrak{p}$ ein Primideal, so ist $(n(\mathfrak{p})) = \mathfrak{p}\cdot\mathfrak{p}'$ ein rationales Hauptideal. Zerlegt man die Zahl $n(\mathfrak{p})$ in ihre Primfaktoren $n(\mathfrak{p}) = p\cdot q \ldots r$, so muß ja, da $\mathfrak{p}\mathfrak{p}'$ in $(n(\mathfrak{p}))$ aufgeht, auch $\mathfrak{p}$ in $n(\mathfrak{p})$ und entweder in (p) oder in $(q \ldots r)$ aufgehen. Im ersten Fall ist der Satz bewiesen; geht aber $\mathfrak{p}$ in $(q \ldots r)$ auf, so muß es entweder in (q) oder in $(\ldots r)$ aufgehen usw. usw., d. h. $\mathfrak{p}$ muß notwendig in *einer* Primzahl, die mit p bezeichnet werden kann, aufgehen. Es kann $\mathfrak{p}$ aber auch nicht gleichzeitig in einer zweiten von p verschiedenen rationalen Primzahl q aufgehen, weil es dann ein Einheitsideal wäre.

$$\varphi(x) = \alpha_0 x^r + \cdots \alpha_r$$

$$\psi(x) = \beta_0 x^s + \cdots \beta_s$$

ganze algebraische Zahlen sind und wenn die Koeffizienten $\gamma_0, \gamma_1 \ldots$ des Produktes beider Funktionen:

$$\varphi(x)\psi(x) = \gamma_0 x^{r+s} + \cdots \gamma_{r+s}$$

sämtlich durch eine ganze algebraische Zahl ω teilbar sind, so ist auch jede der $(r+1)(s+1)$ Zahlen $\alpha_i\beta_k$ durch ω teilbar. (Hurwitz, Gött. Nachr. 1894, S. 291—292.)

Vergl. L. Kronecker: Zur Theorie der Formen höherer Stufen; Werke II, S. 417. Ein einfacher Beweis des allgemeinen Satzes findet sich in: J. König, Einleitung in die allgemeine Theorie der algebraischen Größen. Leipzig 1903. § 5 u. flg. S. 78.

1) Nachr. der K. Ges. d. Wissensch. zu Göttingen. Math. phys. Klasse. 1894, S. 291 ff.

2) Math. Annalen, Bd. 44, Jahrg. 1894, S. 1 und Jahresb. der Deutsch. Math.-Vereinig., 3. Bd., 1893, S. 59.

Ebenso wie $\mathfrak{p}$ in (p) aufgeht, so geht auch $\mathfrak{p}'$ in (p) und in keiner anderen rationalen Primzahl auf.

Man beachte übrigens, daß ein solches Primideal $\mathfrak{p}$ nur rationale Zahlen enthalten kann, die Vielfache von p sind, und nur solche Körperzahlen α, deren Norm $n(\alpha)$ durch p teilbar ist.

Ist nun $\mathfrak{a}$ ein Ideal, so ist es ein Primideal *ersten* oder *zweiten Grades*, je nachdem $n(\mathfrak{a})$ entweder gleich einer Primzahl p oder gleich p^2 ist.

Die Primfaktoren eines beliebigen Ideals $\mathfrak{a}$ ergeben sich hiernach, indem man zuerst $n(\mathfrak{a})$ bildet und dann diese rationale Zahl in ihre rationalen Primfaktoren und diese schließlich in Primideale zerlegt.

Um ein Ideal zu geben, z. B. ein solches, welches in einer Primzahl p aufgeht, kann man natürlich nicht unendlich viele Zahlen bestimmen. Tatsächlich ist ja auch ein Hauptideal schon durch eine Zahl gegeben, und ein beliebiges Nichthauptideal kann schon durch zwei Zahlen gegeben sein, welche nicht notwendig eine Basis des Ideals zu bilden brauchen.

Mit Rücksicht hierauf führen wir noch folgenden Satz an:

Satz. *Jedes Ideal* $\mathfrak{j}$ *kann dargestellt werden durch* (α, β) *als größter gemeinsamer Teiler der ganzen Zahlen* α, β.

Man wähle aus dem Ideal zwei Zahlen α, β, oder aus dem Körper zwei ganze Zahlen α, β, die durch $\mathfrak{j}$ teilbar sind, so aus, daß $\frac{(\alpha)}{\mathfrak{j}}$ und $\frac{(\beta)}{\mathfrak{j}}$ prim zueinander ausfallen, dann ist $\mathfrak{j} = (\alpha, \beta)$.

14. Die Faktoren der rationalen Primzahlen im Körper $k(\sqrt{m})$.

Ein Primideal $\mathfrak{p}$, das also stets in einer rationalen Primzahl p aufgehen muß, kann, wie schon früher gezeigt wurde, nur von einer der folgenden Formen sein:

$$1.)\ \mathfrak{p} = (p, a + \omega) \quad \text{oder} \quad 2.)\ \mathfrak{p} = (p, p\omega).$$

Im erstern Fall ist $(p) = \mathfrak{p}\mathfrak{p}'$ und (p) also zerlegbar in ein Produkt aus zwei Primidealen ersten Grades, im letztern Fall ist $\mathfrak{p} = (p)$, und (p) ist nicht zerlegbar, sondern stellt selbst ein Primideal, zweiten Grades, dar.

Um bei einer gegebenen Zahl m die Frage zu entscheiden, welche rationalen Primzahlen im Körper $k(\sqrt{m})$ zerlegbar sind, soll ein einfaches Kriterium aufgestellt werden, durch welches diese Frage für jede gegebene Primzahl p auf eine kurze Rechnung zurückgeführt wird.

1. Fall. $m \equiv 3$, (4), Körperdiskriminante $d = 4m$.

Es stelle p eine beliebige Primzahl vor, welche nur nicht in der Körperdiskriminante $d = 4m$ aufgehen soll, also insbesondere sei p verschieden von 2. Ist p im Körper k zerlegbar, so ist:

$$\mathfrak{p} = (p,\ a + \sqrt{m}),$$

und es muß a der Kongruenz genügen:

$$(a + \sqrt{m})(a - \sqrt{m}) = a^2 - m \equiv 0,\ (p).$$

Umgekehrt, wenn die Kongruenz

$$x^2 - m \equiv 0,\ (p) \tag{C}$$

eine ganzzahlige rationale Lösung $x = a$ besitzt, so ist p in zwei verschiedene Primideale ersten Grades zerlegbar.

Denn ist $x = a$ eine Lösung der Kongruenz (C) (aber nicht eine solche der Kongruenz $x^2 - m \equiv 0,\ (p^2)$), so sind $\mathfrak{p} = (p,\ a + \sqrt{m})$ und $\mathfrak{p}' = (p,\ a - \sqrt{m})$ zwei in (p) aufgehende Ideale. Dieselben sind verschieden, da unter Berücksichtigung des Umstandes, daß a prim ist zu p, der größte gemeinsame Teiler von $\mathfrak{p}$, $\mathfrak{p}'$, nämlich $(p,\ a + \sqrt{m},\ a - \sqrt{m},\ 2a,\ 1)$ ein Einheitsideal ist, und da weder $\mathfrak{p}$ noch $\mathfrak{p}'$ für sich ein Einheitsideal ist. Schließlich sind $\mathfrak{p}$ und $\mathfrak{p}'$ auch von (p) verschieden, weil p weder in $a + \sqrt{m}$ noch in $a - \sqrt{m}$ aufgehen kann und es besteht die Gleichung $(p) = \mathfrak{p}\mathfrak{p}'$.

Die Tatsache, daß die Kongruenz (C) eine Lösung besitzt, und zwar soll als solche stets ein Wert a genommen werden, für welchen zugleich $a^2 - m \not\equiv 0,\ (p^2)$ ist, bezeichnet man kurz damit, daß das *Legendresche Symbol* $\left(\frac{m}{p}\right) = 1$ gesetzt wird.

Unter der Voraussetzung $p > 2$ besitzt die Kongruenz $x^2 - m \equiv 0,\ (p)$ eine Lösung sicher dann, wenn auch die andere Kongruenz $y^2 - 4m \equiv 0,\ (p)$ oder $y^2 - d \equiv 0,\ (p)$ eine Lösung besitzt. Denn unter den ev. Lösungen dieser letztern befinden sich sicher auch *gerade* Zahlen y und man braucht dann nur $x = \frac{1}{2}y$ zu nehmen.

Statt $\left(\frac{m}{p}\right) = 1$ kann man daher auch $\left(\frac{d}{p}\right) = +1$ schreiben.

Ist die Kongruenz $x^2 - m \equiv 0,\ (p)$ oder die ihr gleichwertige $y^2 - 4m \equiv 0,\ (p)$ nicht lösbar, so ist p im Körper $k(\sqrt{m})$ unzerlegbar, ergibt also selbst ein Primideal zweiten Grades. Man drückt dies kurz damit aus, daß man setzt:

$$\left(\frac{m}{p}\right) = \left(\frac{4m}{p}\right) = \left(\frac{d}{p}\right) = -1.$$

Nun bleiben noch diejenigen Primzahlen zur Betrachtung übrig, welche in der Körperdiskriminante aufgehen, nämlich erstens die Primzahl $p = 2$ und die ungeraden (einfachen) Primfaktoren von m.

Die Kongruenz

$$x^2 - m \equiv 0, \ (2)$$

ist sofort durch $x = +1$ oder $x = -1$ gelöst, zwei Lösungen, die aber mod. (2) gleich sind.

Man hat daher als Primideale, welche in (2) aufgehen:

$$\mathfrak{p} = (2, \ 1 + \sqrt{m}) \quad \text{oder} \quad \mathfrak{p}' = (2, \ 1 - \sqrt{m}).$$

In diesem Fall sind jedoch, anders als im Falle eines beliebigen p, die beiden Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ nicht verschieden sondern gleich; es ist

$$(2, \ 1 + \sqrt{m}) = (2, \ 1 + \sqrt{m}, \ 1 - \sqrt{m}) = (2, \ 1 - \sqrt{m}),$$

oder

$$\mathfrak{p} = \mathfrak{p}'.$$

Da $\mathfrak{p}$ kein Einheitsideal ist und 2 auch nicht in $1 + \sqrt{m}$ aufgeht, so ist also (2) im Körper $k(\sqrt{m})$ das Quadrat eines Primideals, gleich $\mathfrak{p}^2$.

Schließlich sei p eine ungerade Primzahl, die in m aufgeht (und zwar nur zur ersten Potenz nach der Voraussetzung über m). Dann besitzt die Kongruenz

$$x^2 - m \equiv 0, \ (p)$$

die Lösung $x = 0$, und es ist p teilbar durch

$$\mathfrak{p} = (p, \ \sqrt{m}) \quad \text{und} \quad \mathfrak{p}' = (p, \ -\sqrt{m}).$$

Die Ideale $\mathfrak{p}$ und $\mathfrak{p}'$ sind aber offenbar identisch, verschieden von (1) und von (p) und:

$$\mathfrak{p} \cdot \mathfrak{p}' = \mathfrak{p}^2 = (p^2, \ p\sqrt{m}, \ m, \ p) = (p).$$

Es ist sonach *jede* in der Körperdiskriminante d aufgehende rationale Primzahl durch das Quadrat eines Primideals teilbar.

Ist p eine in d aufgehende Primzahl, oder hat die Kongruenz $y^2 - d \equiv 0, \ (p)$ nur eine Lösung $y \equiv 0, \ (p)$, so kann man dies dadurch ausdrücken, daß man die bisherige Bedeutung des Legendreschen Symbols erweitert, indem man jetzt $\left(\frac{d}{p}\right) = 0$ setzt.

2. Fall. $m \equiv 2, \ (4)$, Körperdiskriminante $d = 4m$. Man findet genau wie im 1. Fall, daß eine Primzahl, welche nicht in der Körperdiskriminante aufgeht, zerlegbar ist oder nicht, je nachdem:

$$\left(\frac{d}{p}\right) = +1, \quad \text{oder} \quad \left(\frac{d}{p}\right) = -1.$$

Ferner ergibt sich für $p = 2$ die Zerlegung:

$$(2) = (2, \sqrt{m})^2 = \mathfrak{p}^2,$$

und für eine ungerade Primzahl, welche in d resp. m aufgeht:

$$(p) = (p, \sqrt{m})^2 = \mathfrak{p}^2.$$

In diesen beiden Fällen besitzt die Kongruenz $x^2 - d \equiv 0,\ (p)$, die doppelt zu zählende Lösung $x = 0$, und man setzt wieder $\left(\frac{d}{p}\right) = 0$.

3. Fall. $m \equiv 1,\ (4)$, Körperdiskriminante $d = m$. Es sei zuerst wieder p eine ungerade Primzahl, welche nicht in der Körperdiskriminante aufgeht.

Falls p zerfällt, so ist ein Primfaktor desselben

$$\mathfrak{p} = (p,\ a + \omega),$$

und es ist daher $(a + \omega)(a + \omega') = \left(a + \frac{1}{2}\right)^2 - \frac{m}{4}$ teilbar durch p. Ist aber $\left(a + \frac{1}{2}\right)^2 - \frac{m}{4}$ durch p teilbar, so ist es auch $4\left[\left(a + \frac{1}{2}\right)^2 - \frac{m}{4}\right]$ und umgekehrt. Es ist folglich eine *notwendige* Bedingung für die Zerlegbarkeit von p, daß die Kongruenz

$$x^2 - d \equiv 0,\ (p)$$

lösbar ist, d. h. daß $\left(\frac{d}{p}\right) = +1$ wird.

Wenn umgekehrt $\left(\frac{d}{p}\right) = +1$ ist, die Kongruenz $x^2 - d \equiv 0,\ (p)$ also lösbar ist, so kann als eine Lösung stets eine ungerade Zahl $2a + 1$ angenommen werden, und dann sind

$$\mathfrak{p} = (p,\ a + \omega) \quad \text{und} \quad \mathfrak{p}' = (p,\ a + \omega')$$

zwei voneinander verschiedene, in p aufgehende Primideale. In der Tat ist der größte gemeinsame Teiler von $\mathfrak{p}$, $\mathfrak{p}'$:

$$(p,\ a + \omega,\ a + \omega',\ 2a + 1,\ 1) = (1),$$

weil $2a + 1$ prim ist zu p. Ferner ist weder $\mathfrak{p}$ noch $\mathfrak{p}'$ gleich (1) oder (p), denn p geht nicht in $a + \omega$ oder $a + \omega'$ auf.

Es sei zweitens $p = 2$.

Wenn dann (2) durch ein Primideal $\mathfrak{p} = (2,\ a + \omega)$ teilbar ist, so ist $(a + \omega)(a + \omega') = \left(a + \frac{1}{2}\right)^2 - \frac{m}{4}$ gerade, oder $(2a + 1)^2 - m$ teilbar durch 8, d. h. es muß die Kongruenz

$$x^2 - m \equiv 0,\ (8)$$

lösbar sein.

Falls umgekehrt diese Kongruenz Lösungen besitzt, können dieselben nur ungerade Zahlen sein, und wenn $2a + 1$ eine solche Lösung bezeichnet, so stellen wiederum

$$\mathfrak{p} = (2,\ a + \omega) \quad \text{und} \quad \mathfrak{p}' = (2,\ a + \omega')$$

zwei verschiedene Primideale dar, welche in (2) aufgehen. In der Tat sind $\mathfrak{p}$ und $\mathfrak{p}'$ verschieden von (2) und verschieden voneinander, denn es ist ihr größter gemeinsamer Teiler:

$$(2, a + \omega, a + \omega', 2a + 1, 1) = (1).$$

Bezeichnet man, unter der wesentlichen Voraussetzung $d \equiv 1, (2)$, mit $\left(\frac{d}{2}\right) = +1$ oder -1 die Tatsache, daß die Kongruenz $x^2 - d \equiv 0, (8)$ Lösungen besitzt oder nicht, so ist $p = 2$ in $k(\sqrt{m})$ zerlegbar oder unzerlegbar, je nachdem $\left(\frac{d}{2}\right) = +1$ oder $\left(\frac{d}{2}\right) = -1$ wird.

Man findet übrigens leicht, daß $\left(\frac{d}{2}\right) = +1$ ausfällt, wenn $m \equiv 1, (8)$ ist, und $\left(\frac{d}{2}\right) = -1$, wenn $m = 5, (8)$ ist.

Es sei schließlich p eine ungerade Primzahl, welche in d resp. m aufgeht, dann genügt $x \equiv 0, (p)$ als Doppelwurzel der Kongruenz $x^2 - d \equiv 0, (p)$, und man setzt wieder $\left(\frac{d}{p}\right) = 0$. Nun stellen $\mathfrak{p} = (p, \sqrt{m})$ oder $\mathfrak{p}' = (p, -\sqrt{m})$ Primideale vor, welche in p aufgehen. Da offenbar wieder $\mathfrak{p} = \mathfrak{p}'$ ist, so wird:

$$(p) = \mathfrak{p}^2.$$

Als Basis des Primideals $\mathfrak{p}$ kann gewählt werden:

$$\iota_1 = p,\ \iota_2 = \frac{p-1}{2} + \omega.$$

Es zeigt sich also auch für den letzten jetzt behandelten Fall wieder, daß alle in der Körperdiskriminante aufgehenden rationalen Primzahlen gleich dem Quadrat eines Primideals sind.

Die Zusammenfassung der drei verschiedenen Fälle liefert nun die folgende Tatsache[1]):

Satz. *Eine rationale Primzahl p ist in dem Zahlkörper $k(\sqrt{m})$ mit der Körperdiskriminante d entweder zerlegbar in das Produkt von zwei konjugierten aber verschiedenen Primidealen, oder gleich dem Quadrat eines Primideals, oder endlich unzerlegbar, je nachdem entweder $\left(\frac{d}{p}\right) = +1$, oder $\left(\frac{d}{p}\right) = 0$, oder $\left(\frac{d}{p}\right) = -1$ ausfällt.*

---

1) Hilbert, Zahlber. § 61, S. 284.

Wenn auch die Berechnung des Symbols $\left(\frac{d}{p}\right)$ erst später als Anwendung des quadratischen Reziprozitätsgesetzes gelehrt werden kann, so ist es hier doch schon möglich, einige Beispiele auszuführen.

Körper $k(\sqrt{-5}),\quad m=-5,\quad d=-20.$

Die Zahlen 2 und 5 sind die einzigen Primfaktoren der Diskriminante, und diese Zahlen müssen daher durch Quadrate von Primidealen teilbar sein.

In der Tat ist:

$$(2)=(2,\ 1+\sqrt{-5})^2,\quad (5)=(\sqrt{-5})^2.$$

Die Kongruenz $x^2+5\equiv 0,\ (p)$ ist lösbar für die ungeraden Primzahlen $p=3,\ 7,\ 23$ usw. und unlösbar für $p=11,\ 13,\ 17,\ 19$ usw. Es ergeben sich daher die Zerlegungen:

$$(3)=(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5});$$
$$(7)=(7,\ 3+\sqrt{-5})(7,\ 3-\sqrt{-5});$$
$$(23)=(23,\ 8+\sqrt{-5})(23,\ 8-\sqrt{-5}),$$

in Primideale ersten Grades, während (11), (13), (17), (19) Primideale zweiten Grades darstellen.

Körper $k(\sqrt{35}),\quad m=35,\quad d=140.$

Die Primzahlen, welche in der Körperdiskriminante aufgehen, sind 2, 5, 7, und daher wird:

$$(2)=(2,\ 1+\sqrt{35})^2;$$
$$(5)=(5,\ \sqrt{35})^2;$$
$$(7)=(7,\ \sqrt{35})^2.$$

Da die Kongruenz $x^2-35\equiv 0,\ (p)$ lösbar ist für $p=13, 17, 19$ usw. und unlösbar für $p=3,\ 11$ usw., so ergeben sich jetzt die Zerlegungen:

$$(13)=(13,\ 3+\sqrt{35})(13,\ 3-\sqrt{35});$$
$$(17)=(17,\ 1+\sqrt{35})(17,\ 1-\sqrt{35});$$
$$(19)=(19,\ 4+\sqrt{35})(19,\ 4-\sqrt{35}),$$

in Primideale ersten Grades. (3), (11) sind dagegen Primideale zweiten Grades.

15. Fundamentalsatz von den linearen Formen.

Es ist notwendig, an dieser Stelle einen Satz zu entwickeln, welcher im folgenden sehr oft zur Anwendung kommt und den man

Herrn Minkowski verdankt. Dieser Satz liefert für eine ganze Klasse von zahlentheoretischen Untersuchungen ein fundamentales und einheitliches Prinzip, wie Herr Minkowski in seinem äußerst interessanten Buch: „Geometrie der Zahlen", 1. Lieferung, Leipzig 1896, auf das ich hier gerne verweise, näher ausgeführt hat.

Zuerst mögen kurz einige sonst gebräuchliche Benennungen erklärt werden: *Homogene lineare Form* mit n Veränderlichen heißt ein Ausdruck:

$$f = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n,$$

in welchem $a_1, a_2, \ldots a_n$ konstante Koeffizienten und $x_1, x_2, \ldots x_n$ veränderliche Größen sind. Liegt ein System von n homogenen linearen Formen mit n Veränderlichen vor:

$$f_i = a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n, \quad (\text{für } i = 1, 2, \ldots n),$$

so heißt die Determinante der n^2 Koeffizienten dieser Formen:

$$\Delta = (a_{11}, a_{22}, \ldots a_{nn}),$$

abgekürzt *die Determinante der n Formen.*

In diesen Bezeichnungen lautet der Satz von Herrn Minkowski:

Satz I.[1]) *Sind* $f_i = a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n$ *(für* $i = 1, 2, \ldots n$*)* n *homogene lineare Formen mit reellen Koeffizienten* a_{ik} *und der Determinante* $+1$, *so kann man stets* n *ganze rationale Zahlen, welche nicht alle gleich Null sind, für* x_1 *bis* x_n *so bestimmen, daß der absolute Wert jeder der Formen* $f \leq +1$ *wird, d. i. daß gleichzeitig*

$$|f_1| \leq 1, \quad |f_2| \leq 1, \ldots \quad |f_n| \leq 1$$

wird.

Den folgenden Beweis für den Satz I hat mir Herr Geheimrat Hilbert in freundlichster Weise zur Verfügung gestellt. Herr Hilbert hat diesen Beweis in einer Vorlesung, gehalten an der Uni-

---

1) H. Minkowski, Geom. d. Zahlen, p. 104. Bei Herrn Minkowski ist dieser Satz ein Spezialfall eines allgemeinen geometrischen Satzes über nirgends konkave Körper mit Mittelpunkt im n-dimensionalen Raum. Ich kann es mir nicht versagen, von diesem tiefgehenden schönen Satz wenigstens eine Spezialisierung auf die Ebene hier mitzuteilen, indem ich den Begriff des Zahlengitters vorausnehme, welcher im 3. Abschnitt erklärt wird:

In einem Zahlengitter, dessen Grundmasche den Inhalt 1 besitzt, sei eine nirgends konkave (sich selbst nicht schneidende) geschlossene beliebige Linie (also auch z. B. ein Polygon) eingezeichnet, so daß ein Gitterpunkt Mittelpunkt dieser Linie ist, und dieselbe ein einfach zusammenhängendes Flächengebiet begrenzt. Wenn alsdann der Flächeninhalt dieses Gebietes gleich 4 ist, so muß innerhalb oder auf der Begrenzungslinie dieses Gebietes mindestens noch ein Gitterpunkt gelegen sein, außer dem Mittelpunkt. Vergl. Minkowski, l. c. p. 76.

versität Königsberg, Winter 1890/91, mitgeteilt. Ich beschränke mich bei der Wiedergabe des Beweises auf den Fall $n = 3$, einmal, weil der Minkowskische Satz nur für $n = 2$ und $n = 3$ in diesem Buch zur Anwendung gelangt, und weil außerdem die allgemeinen Prinzipien der Beweismethode auch schon für $n = 3$ voll zur Geltung kommen.

Beweis. Der Beweis wird in drei Schritten geführt.

1. Es möge als *Normalform* für drei Formen f_1, f_2, f_3 das System

$$f_1 = \frac{x_1}{h_1}, \quad f_2 = \frac{x_2}{h_2}, \quad f_3 = c_1 x_1 + c_2 x_2 + h_1 h_2 x_3$$

bezeichnet werden, falls h_1 und h_2 ganze rationale und c_1, c_2 beliebige reelle Zahlen sind. Dabei bedeutet es keine Beschränkung, wenn man ferner h_1, h_2 positiv annimmt, weil man sonst nur x_i durch $-x_i$ zu ersetzen braucht. Nun wird zuerst gezeigt, daß der Satz für die Normalform gültig ist. Setzt man für x_1 eine Zahl des Systems $0, \pm 1, \pm 2, \ldots \pm \frac{h_1}{2}$ oder des andern: $0, \pm 1, \pm 2, \ldots \pm \frac{h_1 - 1}{2}, \left[\frac{h_1}{2}\right] + 1$, je nachdem h_1 eine gerade oder ungerade Zahl ist, und setzt ferner zugleich für x_2 eine der Zahlen $0, \pm 1, \pm 2, \ldots \pm \frac{h_2}{2}$, oder $0, \pm 1, \pm 2, \ldots \pm \frac{h_2 - 1}{2}, \left[\frac{h_2}{2}\right] + 1$, je nachdem wieder h_2 gerade oder ungerade ist, so erhält man $(h_1 + 1)(h_2 + 1)$ Kombinationen von Werten x_1, x_2, für welche $|f_1| \leq \frac{1}{2}$ resp. $\leq \frac{1}{2} + \frac{1}{2h_1}$ und $|f_2| \leq \frac{1}{2}$ resp. $\leq \frac{1}{2} + \frac{1}{2h_2}$ ist. Für jede dieser Wertekombinationen x_1, x_2 kann man sodann die dritte Veränderliche x_3 als ganze rationale Zahl so wählen, daß $f_3 = h_1 h_2 \left(\frac{c_1 x_1 + c_2 x_2}{h_1 h_2} + x_3\right)$ ein Wert zwischen 0 und $h_1 h_2$ ist. In der Tat kann man doch x_3 so wählen, daß $\frac{c_1 x_1 + c_2 x_2}{h_1 h_2} + x_3$ ein positiver Bruch zwischen 0 und 1 ist, dann wird $0 < f_3 \leq h_1 h_2$. Denkt man sich nun die $(h_1 + 1)(h_2 + 1)$ Werte von f_3 ihren resp. Größen entsprechend den Zahlenintervallen 0 bis 1; 1 bis 2; 2 bis 3 usw. und $h_1 h_2 - 1$ bis $h_1 h_2$ zugeteilt, dann verteilen sich $(h_1 + 1)(h_2 + 1)$ Werte f_3 auf $h_1 h_2$ Intervalle, es muß daher in *mindestens* einem Intervalle mehr als ein Wert f_3 liegen. Nehmen wir an für $x_i = a_i$ und $x_i = a_i'$ liegen die Werte $f_3' = c_1 a_1 + c_2 a_2 + h_1 h_2 a_3$ und $f_3'' = c_1 a_1' + c_2 a_2' + h_1 h_2 a_3'$ in einem Intervall, so ist offenbar $|f_3' - f_3''| \leq 1$, oder $|f_3| \leq 1$ für die nicht verschwindenden Differenzen $x_i = a_i - a_i'$, $(i = 1, 2, 3)$. Mit Rücksicht auf die Bestimmung der Werte a_1, a_2, a_1', a_2' ist dann gleichzeitig $|a_1 - a_1'| \leq h_1, |a_2 - a_2'| \leq h_2$, folglich

ergeben sich für $x_1 = a_1 - a_1'$ und $x_2 = a_2 - a_2'$ auch die Werte: $|f_1| \leq 1$, $|f_2| \leq 1$. Damit ist der Satz für die Normalform bewiesen.

2. Sind nun:

$$f_i = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 \text{ (für } i = 1, 2, 3) \qquad \text{(I)}$$

drei lineare Formen mit ganz beliebigen reellen Koeffizienten und der Determinante $\Delta = +1$, so liegt der Gedanke nahe, daß man durch eine Transformation von folgender Art:

$$x_i = l_{i1}y_1 + l_{i2}y_2 + l_{i3}y_3 \quad \text{(für } i = 1, 2, 3), \qquad \text{(S.)}$$

die ursprünglichen Formen in die Normalform überführt. Setzt man die Werte x_i in die Formen f_i ein, so erhält man die transformierten Formen in den Veränderlichen y mit einer Determinante Δ_y, welche sich nach dem Produktsatz für Determinanten berechnet zu:

$$\Delta_y = (a_{11}, a_{22}, a_{33}) \cdot (l_{11}, l_{22}, l_{33}) = 1 \cdot (l_{11}\, l_{22}\, l_{33}).$$

Damit auch die Determinante der transformierten Formen $\Delta_y = 1$ wird, muß jedenfalls die Substitution (oder Transformation) (S) eine „Einheitstransformation“ sein, d. h. $(l_{11}\, l_{22}\, l_{33}) = +1$ ausfallen.

Bedeuten außerdem die Koeffizienten l_{ik} ganze rationale Zahlen mit der Determinante $(l_{11}, l_{22}, l_{33}) = 1$, so ergeben sich aus den Formeln (S) ganzzahlige Werte von y zu ganzzahligen x und umgekehrt. Damit die Einheitstransformation (S) die Form f_1 in $\frac{y_1}{h_1}$ überführt, müssen die Koeffizienten l_{ik} folgende Gleichungen erfüllen:

$$(l_{11}\, l_{22}\, l_{33}) = 1 \qquad (1)$$

$$a_{11}\, l_{11} + a_{12}\, l_{21} + a_{13}\, l_{31} = \frac{1}{h_1} \qquad (2)$$

$$a_{11}\, l_{12} + a_{12}\, l_{22} + a_{13}\, l_{32} = 0 \qquad (3)$$

$$a_{11}\, l_{13} + a_{12}\, l_{23} + a_{13}\, l_{33} = 0. \qquad (4)$$

Es ließen sich nun wohl die Größen l_{ik} als ganze rationale Zahlen diesen Gleichungen entsprechend bestimmen, falls man a_{11}, a_{12}, a_{13} rational und teilerfremd, oder mit einem rationalen gemeinsamen Faktor $\frac{1}{h}$ voraussetzen dürfte. Dieser Voraussetzung brauchen indessen die a im allgemeinen nicht zu genügen, wohl aber genügen ihr andere Formen, welche sich ev. *beliebig wenig* von den gegebenen Formen unterscheiden, woraus sich folgendes Beweisverfahren ergibt:

Es sei $a_{11}\, a_{22} - a_{21}\, a_{12}$ die Unterdeterminante von a_{33} in $(a_{11}\, a_{22}\, a_{33})$, welche nicht verschwindet, und es bedeute δ eine willkürlich gegebene, beliebig kleine positive Größe. Dann kann man stets eine Größe $\varepsilon < \delta$ finden, von der Eigenschaft, daß nach einer Änderung (*Variation*)

der Koeffizienten $a_{11}, a_{12}, \ldots a_{32}$ um Größen $\leqq \varepsilon$, der Koeffizient a_{33} höchstens noch um die Größe δ verändert zu werden braucht, damit die Determinante $\varDelta_v$ der variierten Formen ebenfalls gleich $+1$ wird. In der Tat, variiert man jeden Koeffizienten a_{ik} um $\varepsilon_{ik} < 1$, indem man sich alle ε_{ik} mit Ausnahme von ε_{33} gegeben denkt, so berechnet sich aus der Schlußbedingung $\varDelta_v = 1$ der Wert ε_{33} zu:

$$\varepsilon_{33} = \frac{\pm \varepsilon_{11} A_{11} \pm \varepsilon_{12} A_{12} + \cdots}{(a_{11} - \varepsilon_{11}, a_{22} - \varepsilon_{22})},$$

wo A_{11}, A_{12} Zahlen sind, die von den Koeffizienten a und etwa noch von den ε_{ik} abhängen. Bezeichnet ε den größten Wert unter allen den Variationen ε_{ik}, so ist

$$|\varepsilon_{33}| < \frac{\varepsilon A}{|(a_{11}\ a_{22})|},$$

wo nun A eine Größe ist, die nur von den Koeffizienten a und bestimmten Zahlen abhängt. Es wird daher $|\varepsilon_{33}| < \delta$ werden, solange ε der stets erfüllbaren Bedingung genügt $\frac{\varepsilon A}{|(a_{11}\ a_{22})|} < \delta$, und umgekehrt.

Dies vorausgeschickt, verändere man nun zuerst die Koeffizienten a_{11}, a_{12}, a_{13} der ersten Form f_1 um weniger als ε, so daß die variierten Koeffizienten *rationale* Zahlen von der Form:

$$\frac{h_{11}}{h'}, \quad \frac{h_{12}}{h'}, \quad \frac{h_{13}}{h'}$$

sind. Dann multipliziere man Zähler und Nenner dieser Koeffizienten mit einer hinreichend hohen Potenz der ganzen Zahl $h_{11} h_{12} h_{13} = H$ und ersetze die $a_{11}, a_{12}\ a_{13}$ durch

$$\frac{H_{11}}{h_1} = \frac{h_{11} H^n \pm 1}{h' H^n}, \quad \frac{H_{12}}{h_1} = \frac{h_{12} H^n}{h' H^n}, \quad \frac{H_{13}}{h_1} = \frac{h_{13} H^n}{h' H^n},$$

so daß schließlich auch diese neuen Ausdrücke sich von a_{11}, a_{12}, a_{13} um weniger als ε unterscheiden. Da H_{11}, H_{12}, H_{13} sicher keinen gemeinsamen Teiler haben, wende man jetzt auf die variierte Form

$$\varphi_1 = \frac{H_{11}}{h_1} x_1 + \frac{H_{12}}{h_1} x_2 + \frac{H_{13}}{h_1} x_3$$

und die Formen f_2, f_3 die Substitution (S) an, und bestimme die l_{ik} derart, daß $(l_{11}\, l_{22}\, l_{33}) = 1$ wird, und ferner:

$$H_{11} l_{11} + H_{12} l_{21} + H_{13} l_{31} = 1 \qquad (1\text{a})$$

$$H_{11} l_{12} + H_{12} l_{22} + H_{13} l_{32} = 0 \qquad (2\text{a})$$

$$H_{11} l_{13} + H_{12} l_{23} + H_{13} l_{33} = 0 \qquad (3\text{a})$$

ausfällt. In der Tat kann man zunächst $l_{12}, l_{22}, l_{32}, l_{13}, l_{23}, l_{33}$ als

ganze rationale Zahlen stets so bestimmen, daß die Gleichungen (2a) und (3a) erfüllt sind. Dann folgt aus denselben:

$$\begin{aligned} H_{11} &= t(l_{22}l_{33} - l_{23}l_{32}), \\ H_{12} &= t(l_{32}l_{13} - l_{12}l_{33}), \\ H_{13} &= t(l_{12}l_{23} - l_{13}l_{22}), \end{aligned} \tag{4}$$

wo t ein rationaler Proportionalitätsfaktor ist. Weil aber H_{11}, H_{12}, H_{13} teilerfremd sind, kann t bloß der reziproke Wert einer ganzen Zahl sein, und man darf zum Voraus für die l teilerfremde ganze rationale Zahlen voraussetzen derart, daß $t = 1$ wird. Die Gleichung (1a) kann ferner stets durch ganze rationale teilerfremde Zahlen l_{11}, l_{21}, l_{31} erfüllt werden, weil ja die Kongruenz:

$$H_{11}x + H_{12}y - 1 \equiv 0, \ (H_{13}),$$

Lösungen besitzt. Die hiermit bestimmten Werte l_{ik} erfüllen schließlich von selbst die Bedingung $(l_{11}, l_{22}, l_{33}) = 1$, wie man erkennt durch Zusammenfassung der Gleichungen (1a) und (4), wenn in den letzteren $t = 1$ eingeführt ist. Die Transformation (S) habe die drei neuen Formen geliefert:

$$\begin{aligned} f_1' &= \frac{y_1}{h_1}, \\ f_2' &= b_{21}y_1 + b_{22}y_2 + b_{23}y_3, \\ f_3' &= b_{31}y_1 + b_{32}y_2 + b_{33}y_3. \end{aligned} \tag{II}$$

Man bestimme jetzt zunächst weiter ein positives $\varepsilon_1 < 1$ derart, daß einer Variation der Koeffizienten b_{21}, b_{22}, b_{23} um Größen $\leqq \varepsilon_1$ solche Variationen der ursprünglichen Koeffizienten a entsprechen, die $\leqq \varepsilon$ sind. Dann verändert man die b_{21}, b_{22}, b_{23} um Größen $< \varepsilon_1$ und stellt damit eine variierte Form

$$\varphi_2' = \frac{H_{21}}{h_2}y_1 + \frac{H_{22}}{h_2}y_2 + \frac{H_{23}}{h_2}y_3$$

her, in welcher H_{22}, H_{23} teilerfremde und H_{21}, H_{22}, H_{23}, h_2 ganze rationale Zahlen sind, während $\frac{H_{21}}{h_2}$ usw. sich um weniger als ε_1 von den b unterscheiden. Auf die Formen f_1', φ_2', f_3' wende man jetzt eine neue ganzzahlige Substitution (S') an, von folgender Form:

$$\left.\begin{aligned} y_1 &= z_1 \\ y_2 &= m_{21}z_1 + m_{22}z_2 + m_{23}z_3 \\ y_3 &= m_{31}z_1 + m_{32}z_2 + m_{33}z_3 \end{aligned}\right\} \tag{S'}$$

mit der Determinante $m_{22}m_{33} - m_{32}m_{23} = +1$, welche die drei Bedingungen befriedigt:

$$H_{21} + H_{22}\, m_{21} + H_{23}\, m_{31} = 0 \tag{1b}$$

$$H_{22}\, m_{22} + H_{23}\, m_{32} = 1 \tag{2b}$$

$$H_{22}\, m_{23} + H_{23}\, m_{33} = 0. \tag{3b}$$

Aus der ersten Gleichung ergeben sich m_{21}, m_{31} auf unendlich viele Weisen als ganze rationale Zahlen; ferner kann nach der letzten Gleichung $m_{33} = + H_{22}$ $m_{23} = - H_{23}$ gewählt werden. Weil aber H_{22}, H_{23} relativ prim gewählt sind, so lassen sich m_{22}, m_{32} der Gleichung (2b) entsprechend bestimmen, wodurch dann zugleich $m_{22}\, m_{33} - m_{23}\, m_{32} = 1$ wird. Die Substitution (S′) liefert jetzt die neuen drei Formen:

$$\left.\begin{aligned} f_1'' &= \frac{z_1}{h_1}, \\ f_2'' &= \frac{z_2}{h_2}, \\ \varphi_3'' &= c_{31}\, z_1 + c_{32}\, z_2 + c_{33}\, z_3. \end{aligned}\right\} \tag{III′}$$

Indem man an dieser Stelle die Anschauung etwas ändert, kann man aber auch sagen, daß die Formen f_1'' und f_2'' durch die nacheinander angewendeten Substitutionen (S) und (S′) aus zwei Formen φ_1, φ_2 hervorgegangen sind, welche ihrerseits aus den ursprünglichen Formen f_1, f_2 durch Variation der Koeffizienten a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23} um Größen $\leqq \varepsilon$ abgeleitet waren, und wo φ_2 ähnlich beschaffen ist wie φ_1. Variiert man dann auch noch in der dritten ursprünglichen Form f_3 die Koeffizienten um Beträge $\leqq \varepsilon$, δ, so daß die Koeffizienten rational sind und die Determinante der variierten Formen wieder gleich $+1$ ist, so erhält man eine Form φ_3, welche durch die nacheinander angewendeten Substitutionen (S), (S′) in eine Form

$$f_3'' = c_1\, z_1 + c_2\, z_2 + h_1\, h_2\, z_3 \tag{ad III}$$

transformiert wird, weil (S) und (S′) zusammen wieder eine Einheitstransformation bilden, und daher $\Delta_z = +1$ sein muß. f_3'' muß seinerseits aus φ_3'' durch Änderung der Koeffizienten um Beträge $\leqq \varepsilon_2$ hervorgehen. Es ist gezeigt, daß der Minkowskische Satz für die Normalformen f_1'', f_2'', f_3'' gilt. Durch die Substitutionsformeln (S) und (S′) erhält man dann rückwärts Werte x_1, x_2, x_3, für welche der Satz von den variierten Formen φ_1, φ_2, φ_3 gilt, somit fehlt allein noch der Nachweis, daß der Satz auch für die ursprünglichen Formen richtig ist, wenn er für beliebig wenig variierte Formen gilt.

3. Ändert man die Koeffizienten der Formen f_1, f_2, f_3 um Größen $\leqq \delta$, so daß ihre Determinante endlich bleibt, auch nicht Null wird und löst man die Gleichungen $\varphi_i = w_i$ $(i = 1, 2, 3)$ für gegebene Zahlen w_i, die zwischen -1 und $+1$ liegen, nach x auf, so liegen

diese Werte $|x|$ alle unter einer endlichen Größe G. Weil aber unterhalb einer solchen Größe G überhaupt nur eine *endliche* Anzahl ganzer rationaler Zahlen liegen, existiert nur ein *endliches* System ganzzahliger Kombinationen x_1, x_2, x_3, für welche $|\varphi_1| \leqq 1$, $|\varphi_2| \leqq 1$, $|\varphi_3| \leqq 1$ ausfallen.

Angenommen, es bestünden für *keines* dieser Wertsysteme die verlangten Ungleichungen $|f_i| \leqq 1$, vielmehr bestünde jedesmal für mindestens eine der ursprünglichen Formen, etwa für f_k, die Gleichung $|f_k| = 1 + \lambda$, wo λ eine positive Zahl ist, dann setze man $\delta < \frac{\lambda}{3GM}$, wo M der absolute Betrag des absolut größten aller Koeffizienten a_{ik} sein soll und G die oben definierte Bedeutung hat, so müßte jedesmal für die variierte Form φ_k die Ungleichung $|\varphi_k| > 1$ gelten, d. h. der Satz wäre auch für die um Größen $\leqq \delta$ variierten Formen nicht richtig. Für diese ist aber die Richtigkeit des Satzes bewiesen, also gibt es stets ein Wertsystem ganzzahliger rationaler Zahlen, für welche

$$|f_1| \leqq 1, \qquad |f_2| \leqq 1, \qquad |f_3| \leqq 1$$

ausfällt.

Meistens ist der Minkowskische Satz in der folgenden, etwas veränderten Gestalt zu verwenden:

Satz II. *Sind*

$$f_i = a_{i1} x_1 + a_{i2} x_2 + a_{i3} x_3, \quad (i = 1, 2, 3)$$

drei lineare Formen mit reellen Koeffizienten und der positiven Determinante Δ, *und sind ferner* w_1, w_2, w_3 *drei positive Zahlen, deren Produkt* $w_1 \cdot w_2 \cdot w_3 = \Delta$ *ist, die sonst aber ganz beliebig sein dürfen, so kann man stets drei ganze rationale Zahlen* x_1, x_2, x_3 *angeben, für welche gleichzeitig*

$$|f_1| \leqq w_1, \quad |f_2| \leqq w_2, \quad |f_3| \leqq w_3$$

ausfällt.

Die Richtigkeit dieses Satzes folgt ganz unmittelbar aus dem ersten Beweis; man braucht nur

$$f_1 = w_1 \cdot \varphi_1, \quad f_2 = w_2 \cdot \varphi_2, \quad f_3 = w_3 \cdot \varphi_3$$

zu setzen, dann sind φ_1, φ_2, φ_3 drei reelle Formen mit der Determinante $+1$. Es lassen sich mithin drei ganzzahlige Werte x_1, x_2, x_3 angeben, für welche

$$|\varphi_1| \leqq 1, \quad |\varphi_2| \leqq 1, \quad |\varphi_3| \leqq 1$$

werden, und für diese selben Werte der Veränderlichen hat man folglich:

$$|f_1| \leqq w_1, \quad |f_2| \leqq w_2, \quad |f_3| \leqq w_3,$$

wie es der zweite Satz verlangt.

Schließlich folgt durch Auflösung der drei Gleichungen $f_i = c_i$ mit der Determinante $\Delta = 1$ nach den Unbekannten x_1, x_2, x_3 der Satz:

Satz III. *Haben die drei linearen Formen*

$$x_i = A_{i1} c_1 + A_{i2} c_2 + A_{i3} c_3 \quad (\text{für } i = 1, 2, 3)$$

reelle Koeffizienten mit der Determinante $+1$, *so kann man für* c_1, c_2, c_3 *stets reelle Werte zwischen* -1 *und* $+1$ *so bestimmen, daß für dieselben die* x_1, x_2, x_3 *sich als ganze rationale Zahlen ergeben.*

16. Äquivalenz der Ideale und die Idealklassen der Körper.

Definition. *Zwei Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *des Zahlkörpers* k *heißen* **äquivalent** *und man schreibt:*

$$\mathfrak{a} \sim \mathfrak{b},$$

wenn ihr Quotient gleich einer Zahl des Körpers ist, oder wenn man zwei ganze Zahlen in k *angeben kann, so daß*

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha}{\beta} \quad \textit{resp.} \quad (\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$$

wird.

Falls $\mathfrak{a}$ ein Hauptideal bezeichnet, so schreibt man einfach $\mathfrak{a} \sim (1)$.

Aus dieser Definition ergeben sich unmittelbar einige Rechnungsregeln für Äquivalenzen.

1. Wenn $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{b} \sim \mathfrak{c}$ ist, so ist auch $\mathfrak{a} \sim \mathfrak{c}$.

2. Wenn $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{c} \sim \mathfrak{d}$ ist, so ist auch $\mathfrak{a} \cdot \mathfrak{c} \sim \mathfrak{b} \cdot \mathfrak{d}$.

3. Wenn $\mathfrak{a}$ und $\mathfrak{b}$ äquivalente Ideale sind und $\mathfrak{c}$ ein drittes Ideal bedeutet von der Beschaffenheit, daß $\mathfrak{a}\mathfrak{c}$ ein Hauptideal ist, so wird auch gleichzeitig $\mathfrak{b}\mathfrak{c}$ ein Hauptideal.

Kummer hat diesen Satz als Definition der Äquivalenz benützt, und derselbe wird im folgenden auch stets angewendet werden bei der Untersuchung der ev. Äquivalenz zweier gegebener Ideale. In der Tat ist der Satz mit der oben angenommenen Definition gleichbedeutend, denn aus

$$\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c} \sim 1$$

folgt:

$$\mathfrak{a}(n(\mathfrak{c})) \sim \mathfrak{b}(n(\mathfrak{c}))$$

und

$$\mathfrak{a} \sim \mathfrak{b}.$$

4. Wenn $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$ und $\mathfrak{a} \sim \mathfrak{b}$ ist, so ist auch $\mathfrak{c} \sim \mathfrak{d}$.

5. Wenn $\mathfrak{a} \sim \mathfrak{b}$ ist, so ist gleichzeitig $\mathfrak{a}' \sim \mathfrak{b}'$, denn es ist $(n(\mathfrak{a})) \sim (n(\mathfrak{b}))$.

Auf den Begriff der Äquivalenz gründet sich jetzt weiter die folgende Definition:

Definition. *Alle Ideale, welche einem und demselben Ideal äquivalent sind, bilden eine* **Idealklasse.**

Danach wird durch jedes Ideal stets eine Idealklasse bestimmt, welche unendlich viele Ideale enthält. Die Definition findet darin ihre Berechtigung, daß alle Ideale einer Klasse immer nur wieder dieselbe Klasse bestimmen. Alle Hauptideale sind dem Ideal (1) äquivalent und bilden zusammen die *Hauptklasse.*

Es mögen künftig große lateinische Buchstaben $K, K_1, K_2 \ldots$ die Klassen eines Körpers bezeichnen, insbesondere schreibt man die Hauptklasse stets $K = 1$.

Gehört das Ideal $\mathfrak{a}$ der Klasse K, $\mathfrak{a}_1$ der Klasse K_1 an, und ist $\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{a}_1$ ein Ideal der Idealklasse K_2, so heißt K_2 das *Produkt der Klassen K und K_1* und man schreibt symbolisch $K_2 = KK_1$. Man kann also Klassen miteinander multiplizieren, indem dabei insbesondere stets die Identität gilt:

$$K = 1 \cdot K.$$

Wie zu jedem Ideal $\mathfrak{a}$ ein Idealfaktor $\mathfrak{a}_1$, auf unendlich viele Weisen, stets so gefunden werden kann, daß $\mathfrak{a} \cdot \mathfrak{a}_1$ ein Hauptideal wird, so gehört zu jeder Klasse K auch *stets eine und nur eine Klasse K_1* mit der Eigenschaft, daß $K \cdot K_1 = 1$ wird.

Zwei Klassen, welche in dieser Beziehung zu einander stehen, heißen *reziprok,* und man schreibt dann: $K_1 = K^{-1}$ oder $K = K_1^{-1}$.

Endlich kann man noch allgemeiner den Begriff der *Division auf das Rechnen mit Idealklassen* ausdehnen: Eine Idealklasse K des Körpers k heißt durch eine Idealklasse K_1 desselben Körpers *teilbar,* wenn es eine Idealklasse K_2 (in k) gibt, so daß $K = K_1 K_2$ wird.

Die Aufstellung der sämtlichen Idealklassen eines Zahlkörpers ermöglicht die folgende Tatsache:

Fundamentalsatz. *Die Anzahl der Idealklassen eines quadratischen Zahlkörpers ist stets endlich. Es gibt nämlich in jeder Idealklasse mindestens ein Ideal, dessen Norm kleiner oder höchstens gleich* $|\sqrt{d}|$ *ist.*

Dem Beweis dieses Fundamentalsatzes soll noch der folgende Hilfssatz vorausgehen:

Hilfssatz. *In jedem Ideal $\mathfrak{a}$ des Körpers k, mit der Diskriminante d, existiert stets eine Zahl α, deren Norm ihrem absoluten Betrage nach* $\leqq |n(\mathfrak{a})\sqrt{d}|$ *ist.*

Beweis. Das Ideal $\mathfrak{a}$ sei in der kanonischen Darstellung geschrieben: $\mathfrak{a} = (i, i_1 + i_2\omega)$, dann setze man im Falle eines reellen Körpers:

$$\left.\begin{aligned} f_1 &= ix \pm (i_1 + i_2\omega)y \\ f_2 &= ix \pm (i_1 + i_2\omega')y \end{aligned}\right\} \qquad \text{(I)}$$

und im Falle eines imaginären Körpers:

$$\left.\begin{aligned} f_1 &= \frac{1}{\sqrt{2}}\left\{2ix + (2i_1 + i_2[\omega + \omega'])y\right\} \\ f_2 &= \frac{1}{\sqrt{2}\sqrt{-1}}\left\{0 \cdot x \pm i_2(\omega - \omega')y\right\} \end{aligned}\right\} \qquad \text{(I')}$$

mit demjenigen Vorzeichen $\pm$, für welches die Determinante $\varDelta$ dieser Formen $\varDelta = ii_2|\sqrt{d}| = |n(\mathfrak{a})\sqrt{d}|$ wird. Ferner bedeuten im Falle eines reellen Körpers $\varkappa_1$ und $\varkappa_2$ irgend zwei positive reelle Zahlen derart, daß $\varkappa_1 \cdot \varkappa_2 = |n(\mathfrak{a})\sqrt{d}|$ ist, im Falle eines imaginären Körpers sei außerdem $\varkappa_1 = \varkappa_2 = \varkappa$, so gibt es nach dem Minkowskischen Satz (S. 71) ganze rationale, von Null verschiedene, Zahlen x, y, für welche die Bedingungen gelten:

$$|f_1| \leqq \varkappa_1, \quad |f_2| \leqq \varkappa_2.$$

In einem reellen Körper ist dann $\alpha = f_1$ eine Zahl der verlangten Art; denn es ist α eine Zahl des Ideals, $\alpha' = f_2$, und $|n(\alpha)| \leqq |n(\mathfrak{a})\sqrt{d}|$. Im Fall eines imaginären Körpers entspricht $\alpha = \frac{f_1 \pm \sqrt{-1}f_2}{\sqrt{2}}$ dem Satze; denn es ist dann α eine Zahl des Ideals, $\alpha' = \frac{f_1 \mp \sqrt{-1}f_2}{\sqrt{2}}$ und $|n(\alpha)| = \frac{1}{2}|f_1^2 + f_2^2| = \frac{1}{2}(\varkappa_1^2 + \varkappa_2^2) = \varkappa^2 < |n(\mathfrak{a})\sqrt{d}|$.

Anmerkung. Der Satz gilt natürlich auch für ein Hauptideal $\mathfrak{a} = (\alpha)$; es gibt also im Körper k stets eine von 0 und ± 1 verschiedene ganze Zahl λ derart, daß $|n(\lambda)| \leqq |\sqrt{d}|$ ist.

Beweis des Fundamentalsatzes. $\mathfrak{a}$ bezeichne ein Ideal der Klasse A, und α sei eine Zahl dieses Ideals, welche der Bedingung $|n(\alpha)| \leqq |n(\mathfrak{a})\sqrt{d}|$ genügt. Es gibt dann in der zu A reziproken Klasse B ein Ideal $\mathfrak{b}$, für welches das Produkt $\mathfrak{a} \cdot \mathfrak{b} = (\alpha)$ wird. Wegen $n(\mathfrak{a})n(\mathfrak{b}) = |n(\alpha)| \leqq |n(\mathfrak{a})\sqrt{d}|$ folgt daher die Ungleichung $n(\mathfrak{b}) \leqq |\sqrt{d}|$. Es enthält also die Idealklasse B ein Ideal, dessen Norm $\leqq |\sqrt{d}|$ ist, vertauscht man die Klasse B mit der Klasse A, so erhält man das entsprechende Resultat für A.

Nun ist aber $|\sqrt{d}|$ für jede endliche Zahl m selbst endlich, und

da es nur eine endliche Anzahl verschiedener Ideale gibt, deren Norm eine gegebene endliche Größe nicht übersteigt, ist auch die Anzahl der Idealklassen selbst endlich und sicher $< 2\,|\sqrt{d}\,|$.

Die *Klassenanzahl* eines Körpers, für welche dauernd der Buchstabe h verwendet werden soll, ist eine der wichtigsten Konstanten desselben, und es möge nun in einigen Beispielen die praktische Bestimmung dieser Anzahl ausgeführt werden.

Beispiele für die Untersuchung der Äquivalenz von Idealen.

Um zu entscheiden, ob zwei gegebene Ideale äquivalent sind, kann man wie in den folgenden Zahlenbeispielen nach Satz 3 dieser Nummer (S. 72) verfahren.

1. *Im Körper* $k(\sqrt{-5})$ ist:

$$(2,\ 1+\sqrt{-5}) \sim (3,\ 1+\sqrt{-5}) \nsim (1),$$

denn multipliziert man beide Seiten dieser Äquivalenz mit $(3,\ 1-\sqrt{-5})$, so ist

$$(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5}) = (3) \sim 1$$

und

$$(2,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5}) = (1+\sqrt{-5}) \sim 1.$$

Ferner ist

$$(3,\ 1+\sqrt{-5}) \sim (3,\ 1-\sqrt{-5}),$$

denn es ist

$$(3,\ 1+\sqrt{-5})^2 = (2-\sqrt{-5}) \sim 1.$$

2. *Im Körper* $k(\sqrt{-23})$, $\omega = \frac{1+\sqrt{-23}}{2}$ ist:

$$(2,\ \omega) \nsim (2,\ \omega'),$$

denn es ist:

$$(2,\ \omega)^2 = (4,\ 2\omega,\ -6+\omega, \ldots) = (4,\ 2-\omega) \nsim 1,$$

während doch

$$(2,\ \omega)(2,\ \omega') = (2) \sim 1 \text{ ist.}$$

Dagegen ist

$$(3,\ \omega) \sim (2,\ \omega'),$$

denn es ist

$$(3,\ \omega)(2,\ \omega) = (6,\ 3\omega,\ 2\omega,\ \omega^2) = (\omega) \sim 1$$

und

$$(2,\ \omega)(2,\ \omega') = (2).$$

3. *Im Körper* $k(\sqrt{31})$ ist:

$$(3,\ 1+\sqrt{31}) \nsim (3,\ 1-\sqrt{31}),$$

denn es ist

$$(3,\ 1+\sqrt{31})^2 = (9,\ 2-\sqrt{31}) \nsim 1.$$

Dagegen ist

$$(3,\ 1+\sqrt{31}) \sim (5,\ 1+\sqrt{31}),$$

denn es ist

$$(3,\ 1+\sqrt{31})(5,\ 1-\sqrt{31}) = (4+\sqrt{31}),$$

und dann folgt von selbst:

$$(3,\ 1-\sqrt{31}) \sim (5,\ 1-\sqrt{31}).$$

Beispiele zur Berechnung der Klassenanzahl.

Für *die Körper* $k(\sqrt{-1})$, $k(\sqrt{-2})$, $k(\sqrt{-3})$ gilt noch das Euklidische Teilerverfahren. Alle Ideale dieser Körper sind Hauptideale, und somit ist die Klassenanzahl jedesmal $h = 1$.

1a. Für *den Körper* $k(\sqrt{-5})$ ist $m = -5 \equiv 3,\ (4)$, also $d = -20$ und $|\sqrt{d}| < 5$. Die Zahlen 2 und 3 sind im Körper zerlegbar, und zwar ist

$$(2) = (2,\ 1+\sqrt{-5})(2,\ -1+\sqrt{-5}) = \mathfrak{a}\cdot\mathfrak{a}',\ \mathfrak{a} = \mathfrak{a}' \text{ und } n(\mathfrak{a}) = 2$$
$$(3) = (3,\ 1+\sqrt{-5})(3,\ -1+\sqrt{-5}) = \mathfrak{b}\cdot\mathfrak{b}',\ n(\mathfrak{b}) = 3.$$

Nun muß nach dem Endlichkeitssatz jedes Ideal des Körpers mindestens einem der Ideale (1), $\mathfrak{a}$, $\mathfrak{b}$ oder $\mathfrak{b}'$ äquivalent sein, weil dies alle Ideale sind, deren Normen $|\sqrt{d}|$ nicht übersteigen. Da aber schon gezeigt wurde, daß $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{b}' \not\sim (1)$ ist, so ist die Klassenanzahl des Körpers $h = 2$, und die Klassen sind gegeben durch die Ideale (1) und $(2,\ 1+\sqrt{-5})$.

2a. Für *den Körper* $k(\sqrt{-23})$ ist $m \equiv 1,\ (4)$, also $d = -23$ und $|\sqrt{d}| < 5$. Die Zahlen 2, 3, 4 sind in Faktoren aus Nichthauptidealen zerlegbar, und zwar ist:

$$(2) = (2,\ \omega)(2,\ \omega') = \mathfrak{a}\cdot\mathfrak{a}', \text{ und } n(\mathfrak{a}) = 2,$$
$$(3) = (3,\ \omega)(3,\ \omega') = \mathfrak{b}\cdot\mathfrak{b}', \text{ und } n(\mathfrak{a}) = 3.$$

Man findet aber, wie oben gezeigt:

$$\mathfrak{a} \sim \mathfrak{b}',\quad \mathfrak{a}' \sim \mathfrak{b} \quad \text{und} \quad \mathfrak{a}^2 \sim \mathfrak{a}',$$

also ist die Klassenanzahl $h = 3$, und die Klassen lassen sich durch die Ideale (1), $\mathfrak{a}$, $\mathfrak{a}^2$ oder (1), $\mathfrak{b}'$, $\mathfrak{b}'^2$ oder (1), $\mathfrak{a}$, $\mathfrak{a}'$ darstellen.

3a. Für *den Körper* $k(\sqrt{31})$ ist $m \equiv 3,\ (4)$, also $d = 124$ und $|\sqrt{d}| < 12$. Von den Primzahlen unterhalb 12 sind 2, 3, 5 zerlegbar, 7 und 11 unzerlegbar.

$$(2) = (39 + 7\sqrt{31})(37 - 7\sqrt{31})$$
$$(3) = (3,\ 1 + \sqrt{31})(3,\ 1 - \sqrt{31}) = \mathfrak{a} \cdot \mathfrak{a}',\ n(\mathfrak{a}) = 3$$
$$(5) = (5,\ 1 + \sqrt{31})(5,\ 1 - \sqrt{31}) = \mathfrak{b} \cdot \mathfrak{b}',\ n(\mathfrak{b}) = 5.$$

Es ergibt sich, wie oben gezeigt wurde, daß $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}'$, $\mathfrak{b}'$ Nichthauptideale sind und
$$\mathfrak{a} \sim \mathfrak{b},\quad \mathfrak{a}' \sim \mathfrak{b}'.$$

Ferner findet man $\mathfrak{a}^2 \sim \mathfrak{a}'$. Die Zahlen 4, 6, 8, 9, 10 können daher nur auf Ideale führen, welche einem der Ideale $\mathfrak{a}$, $\mathfrak{a}^2$, (1) äquivalent sind. Man behält somit $h = 3$. Die Klassen des Körpers sind gegeben durch die Ideale (1), $\mathfrak{a}$, $\mathfrak{a}^2$, oder 1, $\mathfrak{a}$, $\mathfrak{a}'$ oder 1, $\mathfrak{b}$, $\mathfrak{b}^2$.

Anmerkung. *Praktisch* ist die vorstehend entwickelte Methode zur Bestimmung der Klassenanzahl stets ausreichend, und wenn Vertreter der Klassen verlangt sind, auch theoretisch voll gültig. Es gibt aber zur Bestimmung der Klassenanzahl noch eine theoretisch vollendete analytische Methode der „analytischen Zahlentheorie“. Dieser Zweig der Zahlentheorie ist im wesentlichen von Lejeune Dirichlet[1]) begründet und von Dedekind, Kronecker u. v. a. ausgebaut worden.

Die aufeinanderfolgenden Potenzen eines Nichthauptideals $\mathfrak{a}$
$$\mathfrak{a},\ \mathfrak{a}^2,\ \mathfrak{a}^3,\ \ldots\ \mathfrak{a}^a,\ \ldots$$
sind lauter verschiedene Ideale und bestimmen entsprechende Idealklassen A, A^2, $A^3 \ldots$ Da aber nur endlich viele Idealklassen existieren, so können die Klassen A, A^2, $A^3 \ldots$ bis ins Unendliche nicht alle verschieden voneinander sein. Benennt man mit A^{a+h_1} die *erste* Klasse, welche mit einer der vorhergehenden A^a übereinstimmt, so ist $A^{a+h_1} = A^a$ und $A^{h_1} = 1$, und es gelten jetzt die Behauptungen:

1. die Klassen A, A^2, $\ldots$ A^{h_1} sind alle verschieden voneinander, während weiter
$$A^{1+h_1} = A^1,\quad A^{2+h_1} = A^2 \quad \text{usw. usw.}$$
wird;

2. der kleinste Exponent h_1, für welchen die Gleichung $A^{h_1} = 1$ gilt, ist ein Teiler der Klassenanzahl h.

Bedeuten nämlich n und n_1 zwei ganze Zahlen unterhalb h_1 und setzt man voraus, daß $A^n = A^{n_1}$ ist, so ergibt sich hieraus $A^{n_1 - n} = 1$, wo nun umsomehr $h' = n_1 - n < h_1$ ist. Folglich wäre schon $A^a = A^{a+h'}$ entgegen der Voraussetzung.

1) Vergl. Ges. Werke, Bd. I, p. 357 ff. und 411 ff. Eine zusammenfassende Darstellung enthält: P. Bachmann, Zahlentheorie, Bd. III, Analytische Zahlentheorie, Leipzig 1894. Man vergl. bes. auch den Zahlber. von Hilbert an den betreffenden Stellen, z. B. § 79, S. 79.

Ist durch die Klassen A, A^2, ... A^{h_1} die Gesamtheit der Idealklassen erschöpft, so ist $h_1 = h$. Falls es aber noch andere Idealklassen des Körpers gibt, und falls B den Klassen A bis A^{h_1} nicht angehört, stellen AB, A^2B, ... $A^{h_1}B$ unter sich und von den A verschiedene Klassen vor. Wenn nun die Idealklassen erschöpft sind, so ergibt sich also $h = 2h_1$, wenn aber C eine Klasse ist, welche weder unter den Klassen A noch unter den Klassen A^iB sich befindet, so stellen die Klassen AC, A^2C, ... $A^{h_1}C$ wiederum h_1 neue untereinander verschiedene Klassen vor. Die Fortsetzung des Schlußverfahrens zeigt, daß $h = n \cdot h_1$ ist, wie die zweite Behauptung aussagt.

Eine direkte Konsequenz dieser Tatsache ist der folgende Satz[1]:

Satz. *Wenn p ein Primteiler der Form $X^2 + mY^2$ ist, für irgendwelche ganze Zahlen X, Y (d. h. wenn $X^2 + mY^2$ durch p teilbar ist), so gibt es stets einen ganzzahligen Exponenten e, für welchen die Gleichung*

$$p^e = x^2 + my^2$$

durch ganze rationale Zahlen x, y befriedigt wird.

Eine Reihe von Sätzen der elementaren Zahlentheorie, von welchen wir die bekanntesten auch angeführt haben, lassen sich nun auf die Idealtheorie[2]) übertragen.

17. Die Funktion $\Phi(\mathfrak{a})$.

In der rationalen Zahlentheorie wird die Frage beantwortet nach der Anzahl $\varphi(n)$ aller Zahlen aus dem vollständigen Restsystem nach einer ganzen positiven Zahl n, die relativ prim sind zu n.

Es sei nun $\mathfrak{a}$ irgend ein beliebiges Ideal des Zahlkörpers $k(\sqrt{m})$, dann kann man entsprechend nach der Anzahl aller Zahlen des Körpers aus einem vollständigen Restsystem nach $\mathfrak{a}$ fragen, die zu $\mathfrak{a}$ relativ prim sind, indem die Primfaktoren des Ideals $\mathfrak{a}$ als bekannt vorausgesetzt werden.

Die gesuchte Anzahl soll analog einem früheren Vorgang mit dem Symbol $\Phi(\mathfrak{a})$ bezeichnet werden und für $\mathfrak{a} = (1)$ sei $\Phi(\mathfrak{a}) = 1$.

Zunächst sei $\mathfrak{a} = \mathfrak{p}$ als ein Primideal ersten Grades vorausgesetzt und es werde nach der Anzahl $\Phi(\mathfrak{p})$ gefragt.

Die Zahlen eines vollständigen Restsystems nach $\mathfrak{p}$ können gebildet werden durch die $n(\mathfrak{p})$ Zahlen $0, 1, 2, \ldots p-1$, unter welchen nur 0 nicht prim ist zu $\mathfrak{p}$; es ist also:

---

1) Cfr. Ch. Hermite, Oeuvres, Paris 1905, t. I, p. 274.

2) Dirichlet-Dedekind, Vorles., Supplement XI, S. 564ff., bes. 567—573.

$$\Phi(\mathfrak{p}) = n(\mathfrak{p}) - 1 = n(\mathfrak{p})\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

Zweitens sei $\mathfrak{p}$ ein Primideal zweiten Grades, dann werden die Zahlen eines vollständigen Restsystems durch

$$r + s \cdot \omega$$

gebildet, wenn r und s die Zahlen 0, 1, 2, ... $p - 1$ durchlaufen, was $p^2 = n(\mathfrak{p})$ Kombinationen entspricht. Unter diesen Zahlen ist wieder nur eine, nämlich 0, welche nicht prim ist zu $\mathfrak{p}$, und wir erhalten wieder

$$\Phi(\mathfrak{p}) = n(\mathfrak{p}) - 1 = n(\mathfrak{p})\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

Wenn weiter $\mathfrak{p}$ ein Primideal zweiten Grades ist und $\mathfrak{a} = \mathfrak{p}^k$ angenommen wird, so bilden die Zahlen $r + s\omega$ ein vollständiges Restsystem nach $\mathfrak{p}^k$, wofern für r und s die Zahlen 1, 2, ... p, ... p^k eingesetzt werden, was $p^{2k} = n(\mathfrak{p}^k)$ Kombinationen ergibt, unter diesen Zahlen sind die Zahlen (und nur diese) $a + b\omega$, bei welchen für a und b die Zahlen $1p, 2p, \ldots p^{k-1} \cdot p$ in allen möglichen Kombinationen gesetzt sind, nicht prim zu $\mathfrak{p}^k$. Solche Zahlen sind es aber $p^{k-1} \cdot p^{k-1} = (p^2)^{k-1}$, und daher ergibt sich für $\Phi(\mathfrak{a})$:

$$\Phi(\mathfrak{p}^k) = n(\mathfrak{p}^k) - n(\mathfrak{p}^{k-1}) = n(\mathfrak{p}^k)\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

Ganz dieselbe Form des Resultates ergibt sich durch eine analoge Überlegung für ein Primideal $\mathfrak{p}$ ersten Grades.

Um jetzt zu dem Resultat für den allgemeinen Fall zu gelangen, setzen wir voraus, es sei $\Phi(\mathfrak{a})$ bestimmt für den Fall, daß $\mathfrak{a} = \mathfrak{p}_1^{k_1} \mathfrak{p}_2^{k_2} \ldots \mathfrak{p}_n^{k_n}$ ist, also für den Fall, daß n verschiedene Primfaktoren in $\mathfrak{a}$ enthalten sind und suchen nun $\Phi(\mathfrak{a}_1)$ zu bestimmen, wenn $\mathfrak{a}_1 = \mathfrak{a} \cdot \mathfrak{p}^k$ vorausgesetzt wird, also für den Fall, daß $\mathfrak{a}_1$ einen Primfaktor $\mathfrak{p}$ weiter enthält als $\mathfrak{a}$, wobei $\mathfrak{p}$ prim zu $\mathfrak{a}$ vorausgesetzt ist.

Es sei das Ideal $\mathfrak{a}$ auf die Normalform gebracht:

$$\mathfrak{a} = (a,\ a_1 + a_2\omega)$$

und

$$\mathfrak{p}^k = (i,\ i_1 + i_2\omega),$$

dann sind a und i sicher prim zueinander, da ja $\mathfrak{a}$ und $\mathfrak{p}$ prim zueinander sind, und es wird:

$$\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}^k = (ai,\ \bar{a} + a_2 i_2 \omega),$$

wenn man berücksichtigt, daß

$$n(\mathfrak{a}_1) = n(\mathfrak{a}) \cdot n(\mathfrak{p}^k) = a i a_2 i_2$$

sein muß.

Die Zahlen, welche ein vollständiges Restsystem nach $\mathfrak{a}$ bilden, $r + s\omega$, ergeben sich, indem man für r die Zahlen 1, 2, ... a und für s die Zahlen 1, 2, ... a_2 einsetzt. Ein vollständiges Restsystem nach $\mathfrak{a}_1$, nämlich $\bar{r} + \bar{s}\omega$, ergibt sich desgleichen, indem für $\bar{r}$ die Zahlen 1, 2, ... ai und für $\bar{s}$ die Zahlen 1, 2, ... $a_2 i_2$ gesetzt werden. Unter der Gesamtheit dieser Zahlen finden sich also $ii_2 \cdot \Phi(\mathfrak{a})$ Zahlen, die relativ prim sind zu $\mathfrak{a}$, wie man erkennt, wenn man die Zahlen $\bar{r}$, $\bar{s}$ der Größe nach ordnet und in i resp. i_2 Intervalle von a bezw. a_2 aufeinanderfolgenden Zahlen zerlegt.

Unter diesen $i_1 i_2 \cdot \Phi(\mathfrak{a}) = n(\mathfrak{p}^k)\,\Phi(\mathfrak{a})$ Zahlen befinden sich nun aber auch noch solche Zahlen des vollständigen Restsystems nach $\mathfrak{a}_1$, welche den Faktor $\mathfrak{p}$ einfach oder mehrfach enthalten und gleichzeitig zu $\mathfrak{a}$ prim sind. Die Anzahl dieser Zahlen läßt sich jedoch leicht darstellen, wenn man von den durch $\mathfrak{p}^1$ teilbaren Zahlen des Restsystems ausgeht. Sie ist so groß als die Anzahl derjenigen Zahlen des vollständigen Restsystems nach $\frac{\mathfrak{a}_1}{\mathfrak{p}} = \mathfrak{a}\,\mathfrak{p}^{k-1}$, welche zu $\mathfrak{a}$ relativ prim sind. Solche Zahlen gibt es, wie eben gezeigt wurde: $n(\mathfrak{p}^{k-1})\,\Phi(\mathfrak{a})$.

Es ist folglich:

$$\Phi(\mathfrak{a}_1) = n(\mathfrak{p}^k)\,\Phi(\mathfrak{a}) - n(\mathfrak{p}^{k-1})\,\Phi(\mathfrak{a}),$$

$$\Phi(\mathfrak{a}_1) = \Phi(\mathfrak{a})\,n(\mathfrak{p}^k)\left(1 - \frac{1}{n(\mathfrak{p})}\right).$$

Diese Formel ist eine Rekursionsformel zur Berechnung der Funktion Φ für ein Ideal mit $n + 1$ verschiedenen Primfaktoren, wenn dieselbe für ein Ideal mit n verschiedenen Primfaktoren bekannt ist. Mit Zuhilfenahme der Formel für $\Phi(\mathfrak{p}^k)$ erhält man daraus für $\mathfrak{a} = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\dots\mathfrak{p}_n^{k_n}$ als Resultat die explizite Darstellung:

$$\Phi(\mathfrak{a}) = n(\mathfrak{a})\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right)\left(1 - \frac{1}{n(\mathfrak{p}_2)}\right)\cdots\left(1 - \frac{1}{n(\mathfrak{p}_n)}\right).$$

Aus dieser expliziten Darstellung der Anzahl der zu $\mathfrak{a}$ relativ primen Zahlen eines vollständigen Restsystems ergeben sich leicht wieder folgende Sätze:

Satz. *Ist das Ideal* $\mathfrak{a}$ *in das Produkt* $\mathfrak{a}_1 \cdot \mathfrak{a}_2$ *der beiden zueinander primen Ideale* $\mathfrak{a}_1$ *und* $\mathfrak{a}_2$ *zerlegbar, so ist:*

$$\Phi(\mathfrak{a}) = \Phi(\mathfrak{a}_1) \cdot \Phi(\mathfrak{a}_2).$$

Satz. *Durchläuft* $\mathfrak{t}$ *alle Idealteiler des Ideals* $\mathfrak{a}$, *so ist:*

$$\sum \Phi(\mathfrak{t}) = n(\mathfrak{a}).$$

Beweis. Es sei zuerst $\mathfrak{a} = \mathfrak{p}^k$, dann sind die Ideale $1, \mathfrak{p}, \mathfrak{p}^2, \dots \mathfrak{p}^k$ alle Idealteiler $\mathfrak{t}$ von $\mathfrak{a}$ und somit:

$$\sum \Phi(\mathfrak{t}) = 1 + \Phi(\mathfrak{p}) + \Phi(\mathfrak{p}^2) + \cdots + \Phi(\mathfrak{p}^k),$$

$$\sum \Phi(\mathfrak{t}) = 1 + \left(1 - \frac{1}{n(\mathfrak{p})}\right)\left\{ n(\mathfrak{p}) + n(\mathfrak{p}^2) + \cdots n(\mathfrak{p}^k)\right\}$$

$$= 1 + (n(\mathfrak{p}) - 1)\,\frac{(n(\mathfrak{p}))^k - 1}{n(\mathfrak{p}) - 1} = (n(\mathfrak{p}))^k = n(\mathfrak{p}^k).$$

Wenn nun ganz allgemein $\mathfrak{a} = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\ldots\mathfrak{p}_n^{k_n}$ gesetzt wird, so kann man sagen, daß alle Teiler von $\mathfrak{a}$ sich als die einzelnen Glieder des (ohne weiteres wohl verständlichen) symbolischen Produkts:

$$(1 + \mathfrak{p}_1 + \cdots \mathfrak{p}_1^{k_1})(1 + \mathfrak{p}_2 + \cdots \mathfrak{p}_2^{k_2})\ldots(1 + \mathfrak{p}_n + \cdots \mathfrak{p}_n^{k_n})$$

darstellen lassen. Nach dem vorhergehenden Satz über die Zerlegung der Funktion $\Phi(\mathfrak{a})$ in Faktoren ergibt sich für $\sum\Phi(\mathfrak{t})$ eine im gewöhnlichen Sinn zu verstehende, eigentliche Summe von Funktionen Φ:

$$1 + \sum_1^n \Phi(\mathfrak{p}_i) + \sum_1^n \Phi(\mathfrak{p}_i^2) + \sum_1^n \Phi(\mathfrak{p}_i\mathfrak{p}_k) + \cdots \sum_1^n \Phi(\mathfrak{p}_i^{k_i}),$$

welche dem symbolischen Produkt gleich gebaut ist:

$$\begin{aligned}\sum\Phi(\mathfrak{t}) &= (1 + \Phi(\mathfrak{p}_1) + \cdots \Phi(\mathfrak{p}_1^{k_1}))\\ &\quad\cdot(1 + \Phi(\mathfrak{p}_2) + \cdots \Phi(\mathfrak{p}_2^{k_2}))\\ &\quad\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\\ &\quad\cdot(1 + \Phi(\mathfrak{p}_n) + \cdots \Phi(\mathfrak{p}_n^{k_n}))\\ &= n(\mathfrak{p}_1^{k_1})\cdot n(\mathfrak{p}_2^{k_2})\ldots n(\mathfrak{p}_n^{k_n}) = n(\mathfrak{a}).\end{aligned}$$

Es besteht also für Ideale ein ganz analoger Satz wie für die ganzen rationalen Zahlen.

18. Der Satz von Fermat für Ideale.

Satz. *Es sei $\mathfrak{a}$ ein Ideal des Körpers $k(\sqrt{m})$ und α eine beliebige zu $\mathfrak{a}$ relativ prime ganze Zahl des Körpers, so gilt stets die Kongruenz*

$$\alpha^{\Phi(\mathfrak{a})} \equiv 1,\ (\mathfrak{a}).$$

Beweis. Es seien $\varrho_1, \varrho_2 \ldots \varrho_\nu$ diejenigen $\nu = \Phi(\mathfrak{a})$ Zahlen eines vollständigen Restsystems nach $\mathfrak{a}$, welche zu $\mathfrak{a}$ prim sind, und es sei nun:

$$\left.\begin{aligned}\varrho_1\alpha &\equiv \sigma_1,\ (\mathfrak{a})\\ \varrho_2\alpha &\equiv \sigma_2,\ (\mathfrak{a})\\ &\vdots\\ \varrho_\nu\alpha &\equiv \sigma_\nu,\ (\mathfrak{a}),\end{aligned}\right\} \qquad (C)$$

wo die $\sigma_1 \ldots \sigma_\nu$ wieder Zahlen desselben vollständigen Restsystems seien, dem auch die Zahlen ϱ angehören, so können keine zwei der

Zahlen σ einander nach $\mathfrak{a}$ kongruent sein, denn wenn

$$\sigma_\lambda \equiv \sigma_\mu, \ (\mathfrak{a})$$

wäre, so müßte

$$\alpha(\varrho_\lambda - \varrho_\mu) \equiv 0, \ (\mathfrak{a}),$$

oder, weil α prim zu $\mathfrak{a}$ ist,

$$\varrho_\lambda \equiv \varrho_\mu, \ (\mathfrak{a})$$

sein, was der Voraussetzung über die ϱ widerspricht. Ferner kann keines der Ideale (σ_λ) mit $\mathfrak{a}$ einen Faktor $\mathfrak{t}$ gemeinsam haben, weil dann aus der Idealgleichung

$$(\varrho_\lambda \alpha - \sigma_\lambda) = \mathfrak{t} \cdot \mathfrak{b}$$

folgen würde, daß dieser Faktor auch in $\varrho_\lambda \alpha$, also in ϱ_λ steckt, da α prim ist zu $\mathfrak{a}$ und folglich auch zu $\mathfrak{t}$.

Die Zahlen $\sigma_1, \sigma_2 \ldots \sigma_\nu$ sind daher wieder alle zu $\mathfrak{a}$ primen Zahlen des vollständigen Restsystems und müssen folglich mit den Zahlen $\varrho_1, \ldots \varrho_\nu$, abgesehen von der Reihenfolge, übereinstimmen. Durch Multiplikation der Kongruenzen (C) erhält man dann:

$$\varrho_1 \cdot \varrho_2 \ldots \varrho_\nu \alpha^{\Phi(\mathfrak{a})} \equiv \sigma_1 \cdot \sigma_2 \ldots \sigma_\nu, \ (\mathfrak{a}),$$

und hieraus folgt schließlich:

$$\alpha^{\Phi(\mathfrak{a})} \equiv 1, \ (\mathfrak{a}).$$

Folgerungen. I. Wenn $\mathfrak{p}$ ein Primideal f^{ten} Grades ($f = 1$ oder 2) des Körpers $k(\sqrt{m})$ ist, und α eine durch $\mathfrak{p}$ nicht teilbare ganze Zahl des Körpers bedeutet, so ist stets:

$$\alpha^{p^f - 1} \equiv 1, \ (\mathfrak{p}),$$

und für eine jede beliebige ganze Zahl α gilt die Kongruenz

$$\alpha^{p^f} \equiv \alpha, \ (\mathfrak{p}).$$

II. Wenn α eine durch das Primideal $\mathfrak{p}$ vom Grade f nicht teilbare ganze Zahl bezeichnet, und wenn e die kleinste positive ganze rationale Zahl ist, für welche die Kongruenz besteht:

$$\alpha^e \equiv 1, \ (\mathfrak{p}),$$

so ist e stets ein Teiler von $p^f - 1$.

Beweis. Angenommen e sei selbst kein Teiler von $p^f - 1$, so bezeichne e_1 den größten gemeinsamen Faktor von e und $p^f - 1$, dann ist $e_1 < e$ und es lassen sich zwei ganze rationale Zahlen x, y stets so bestimmen, daß

$$ex + (p^f - 1)y = e_1$$

wird. Nun folgt aus den Kongruenzen, denen α genügt, weiter:

$$\alpha^{ex} \equiv 1, \ (\mathfrak{p})$$

$$\alpha^{(p^f-1)y} \equiv 1, \ (\mathfrak{p})$$

und hieraus

$$\alpha^{ex+(p^f-1)y} \equiv 1, \ (\mathfrak{p}),$$

oder es gilt für den Exponenten e_1 die Kongruenz:

$$\alpha^{e_1} \equiv 1, \ (\mathfrak{p}),$$

es wäre also auch e nicht die kleinste positive Zahl, für welche eine Kongruenz $\alpha^u \equiv 1$, $(\mathfrak{p})$ erfüllt ist und dies widerspricht der Voraussetzung über e. Somit bleibt nur übrig, daß e selbst ein Teiler von $p^f - 1$ ist.

III. Nach einer beliebigen k^{ten} Potenz von $\mathfrak{p}$ gilt für α stets die Kongruenz:

$$\alpha^{p^{fk-f}(p^f-1)} \equiv 1, \ (\mathfrak{p}^k).$$

Wegen einer Anwendung in den folgenden Sätzen führe ich hier gleich die allgemeinen Kongruenzen ein.

Eine ganze Funktion einer Veränderlichen ξ vom Grade g mit ganzen, dem Bereich $k(\sqrt{m})$ angehörigen Koeffizienten kann man in bezug auf ihre Eigenschaften nach einem Idealmodul $\mathfrak{a}$ untersuchen. Man spricht dann von einer Kongruenz mit einer Unbekannten ξ und vom Grade g, wenn der Koeffizient des höchsten Gliedes ξ^g nicht durch $\mathfrak{a}$ teilbar ist. Wenn nun z. B. die Kongruenz:

$$\alpha \xi^g + \alpha_1 \xi^{g-1} + \alpha_2 \xi^{g-2} + \cdots \alpha_g \equiv 0, \ (\mathfrak{a})$$

mit den ganzzahligen Koeffizienten $\alpha, \alpha_1, \ldots \alpha_g$ gegeben ist, so ist eines der Hauptprobleme: die ganzen Zahlen ϱ des Körpers von der Beschaffenheit zu bestimmen, daß die Kongruenz für $\xi = \varrho$ befriedigt ist. Falls ϱ eine solche Zahl ist, so heißt sie eine Wurzel der Kongruenz.

Am einfachsten sind die Kongruenzen nach einem Primidealmodul $\mathfrak{p}$, für welche der folgende einfache Fundamentalsatz gilt:

Satz. *Eine Kongruenz g^{ten} Grades nach dem Modul $\mathfrak{p}$, in welcher der Koeffizient α des höchsten Gliedes prim ist zu $\mathfrak{p}$:*

$$f(\xi) = \alpha \xi^g + \cdots \alpha_g \equiv 0, \ (\mathfrak{p}),$$

kann höchstens g nach $\mathfrak{p}$ inkongruente Wurzeln besitzen.

Beweis. Wenn ϱ_1 eine Wurzel der Kongruenz ist, so ist

$$f(\varrho_1) \equiv 0, \ (\mathfrak{p})$$

und

$$f(\xi) \equiv f(\xi) - f(\varrho_1) = (\xi - \varrho_1) f_1(\xi) \equiv 0, \ (\mathfrak{p}),$$

wo $f_1(\xi)$ vom Grad $g-1$ ist. Sind nun $\varrho_1, \varrho_2 \ldots \varrho_g$ lauter nach $\mathfrak{p}$ inkongruente Wurzeln der Kongruenz, so ist:

$$f(\xi) \equiv \alpha(\xi-\varrho_1)(\xi-\varrho_2)\ldots(\xi-\varrho_g) \equiv 0, \ (\mathfrak{p}).$$

Diese Kongruenz kann für eine ganze Zahl ξ nur befriedigt sein, wenn $\mathfrak{p}$ in *einem* der g Faktoren aufgeht, d. h. wenn etwa $\xi-\varrho_x \equiv 0, (\mathfrak{p})$ ist, und damit ist die Behauptung bewiesen.

19. Primitivzahlen nach einem Primideal.

Es möge α eine durch das Primideal $\mathfrak{p}$ vom Grade f nicht teilbare ganze Zahl sein, z. B. eine Zahl aus dem einfachsten vollständigen Restsystem nach $\mathfrak{p}$, so muß es, wie eben gezeigt wurde, stets einen rationalen Teiler e der Zahl p^f-1 geben, für welchen die Kongruenz

$$\alpha^e \equiv 1, \ (\mathfrak{p})$$

erfüllt ist.

Wenn e der kleinste Exponent ist, für welchen diese Kongruenz gilt, so müssen die Zahlen

$$\alpha, \alpha^2, \alpha^3, \ldots \alpha^{e-1}$$

nach dem Modul $\mathfrak{p}$ alle verschieden sein.

Denn, wenn etwa für zwei verschiedene Zahlen e_1 und e_2 aus der Reihe $1, 2, \ldots p-1$ die Kongruenz:

$$\alpha^{e_1} \equiv \alpha^{e_2}, \ (\mathfrak{p})$$

bestünde, so müßte

$$\alpha^{e_2}(\alpha^{e_1-e_2}-1) \equiv 0, \ (\mathfrak{p}),$$

oder weil α^{e_2} prim zu $\mathfrak{p}$ ist

$$\alpha^{e_1-e_2} \equiv 1, \ (\mathfrak{p})$$

sein. Da aber der Exponent $e_1-e_2<e$ ist, so widerspricht die Annahme der Voraussetzung.

Wenn nun e der kleinste ganzzahlige Exponent ist, so daß

$$\alpha^e \equiv 1, \ (\mathfrak{p}),$$

so soll künftig *α zum Exponenten e gehörig* heißen.

Eine Zahl π des Körpers, welche zum Exponenten p^f-1 gehört [welche also so beschaffen ist, daß $e=p^f-1$ der kleinste Exponent ist, für welchen die Kongruenz gilt:

$$\pi^e \equiv 1, \ (\mathfrak{p})],$$

soll eine **Primitivzahl** nach dem Primideal $\mathfrak{p}$ heißen. Die Potenzen

$$\pi, \pi^2, \pi^3, \ldots \pi^{p^f-1}$$

stellen dann lauter mod $\mathfrak{p}$ verschiedene und zu $\mathfrak{p}$ prime Zahlen des

Körpers, oder die sämtlichen zu $\mathfrak{p}$ relativ primen Zahlen eines vollständigen Restsystems nach $\mathfrak{p}$ dar.

Damit diese Definition einen wirklichen Inhalt hat, ist noch nachzuweisen, daß es nach einem gegebenen beliebigen Primideal $\mathfrak{p}$ stets auch Primitivzahlen gibt. Dieser Nachweis ist möglich, ja durch Verallgemeinerung eines von Gauß zuerst angewandten Beweisverfahrens kann man sogar den folgenden allgemeineren Satz beweisen:

Satz. *Wenn e ein rationaler Primfaktor der ganzen rationalen Zahl p^f-1 ist und $\mathfrak{p}$ ein Primideal vom Grade f bedeutet, das in p aufgeht, so gibt es in einem vollständigen Restsystem nach $\mathfrak{p}$ stets $\varphi(e)$ zum Exponenten e gehörige Zahlen.*

In diesem Satz hat $\varphi(e)$ die in der Einleitung erklärte Bedeutung.

Beweis. Man zeigt zunächst: *wenn* es eine Zahl α gibt, welche zum Exponenten e (also einem Teiler der Zahl p^f-1) gehört, so gibt es mindestens $\varphi(e)$, aber auch *nicht mehr*, nach dem Modul $\mathfrak{p}$ inkongruente Zahlen des Körpers, welche ebenfalls zum Exponenten e gehören.

In der Tat, ist r eine Zahl aus der Reihe $1, 2, \ldots e-1$ *relativ prim zu e*, so muß die Zahl α^r ebenfalls zum Exponenten e und kann zu keinem kleineren Exponenten als e gehören. Aus der Voraussetzung, daß α zum Exponenten e gehöre, folgt: $(\alpha^r)^e \equiv 1$, $(\mathfrak{p})$, denn es ist:

$$(\alpha^r)^e = \alpha^{re} = (\alpha^e)^r \equiv 1, \; (\mathfrak{p}).$$

Da ferner r prim zu e vorausgesetzt ist, so kann überdies die Kongruenz

$$(\alpha^r)^{e_1} \equiv 1, \; (\mathfrak{p})$$

für einen Exponenten e_1 nur bestehen, wenn

$$re_1 \equiv 0, \; (e) \quad \text{oder} \quad e_1 \equiv 0, \; (e)$$

ist, d. h. wenn e_1 durch e teilbar ist, also im äußersten Fall, wenn $e_1 = e$ ist. Setzt man statt r diejenigen Zahlen $r_1, r_2, \ldots r_\nu$ aus der Reihe $1, 2. \ldots e-1$, welche zu e prim sind, so erhält man $\varphi(e)$ verschiedene zum Exponenten e gehörige Zahlen, indem schon gezeigt worden ist, daß die Potenzen $\alpha, \alpha^2, \ldots \alpha^e$ alle mod $(\mathfrak{p})$ inkongruent sind.

Außer diesen Zahlen gibt es aber keine weiteren zum Exponenten e gehörigen Zahlen. Jede derselben muß nämlich der Kongruenz:

$$\xi^e \equiv 1, \; (\mathfrak{p})$$

genügen. Diese Kongruenz wird nun durch die e voneinander mod $\mathfrak{p}$ verschiedenen ganzen Zahlen

$$\alpha, \alpha^2, \alpha^3, \ldots \alpha^e$$

befriedigt und kann, wie oben gezeigt, außerdem *keine weitere* Wurzel besitzen, da sie nie mehr als e nach dem Modul $\mathfrak{p}$ verschiedene Wurzeln überhaupt besitzt. Diejenigen Potenzen α^s, deren Exponenten s mit e einen gemeinsamen Faktor $\bar{e}$ besitzen, gehören alsdann zum Exponenten $\frac{e}{\bar{e}} = e_1 < e$.

Damit ist der erste Schritt zum Beweis des Satzes geschehen: *wenn* es eine Zahl α gibt, welche zu einem Teiler e von $p^f - 1$ gehört, so gibt es im ganzen $\varphi(e)$, und nie mehr, zum Teiler $\mathfrak{p}$ gehörige Zahlen.

Nach dieser Hilfsbetrachtung beweist man die aufgestellte Behauptung vollends leicht folgendermaßen:

Von den $p^f - 1$ inkongruenten Zahlen eines vollständigen Restsystems nach $\mathfrak{p}$ muß jede Zahl zu einem ganz bestimmten Teiler von $p^f - 1$ gehören. Wären nun $t_1, t_2, \ldots t_m$ alle Teiler von $p^f - 1$, zu welchen, als Exponenten genommen, wirklich Zahlen gehören, so müßte die Beziehung bestehen:

$$\varphi(t_1) + \varphi(t_2) + \cdots \varphi(t_m) = n(\mathfrak{p}) - 1 = p^f - 1,$$

da zu jedem Teiler t auch $\varphi(t)$ Zahlen gehören. Nun ist aber

$$\sum \varphi(t) = n(\mathfrak{p}) - 1$$

dann, und nur dann, wenn t *alle* Teiler von $n(\mathfrak{p}) - 1$ durchläuft. Es kann also nicht einen Teiler geben, zu dem keine Zahl gehören würde, und insbesondere gibt es genau $\varphi(n(\mathfrak{p}) - 1) = \varphi(p^f - 1)$ nach $\mathfrak{p}$ inkongruente Primitivzahlen.

Aus dem eben aufgestellten Satz folgt leicht eine Erweiterung eines von Wilson aufgestellten Satzes:

Satz. *Sind $\varrho_1, \varrho_2 \ldots \varrho_\nu$ die inkongruenten Zahlen eines vollständigen Restsystems nach einem in 2 nicht aufgehenden Primideal $\mathfrak{p}$, so ist:*

$$\varrho_1 \cdot \varrho_2 \ldots \varrho_\nu \equiv -1, \ (\mathfrak{p}).$$

Beweis. Sei π eine Primitivzahl nach $\mathfrak{p}$, so kann man setzen:

$$\varrho_1 \equiv \pi^{e_1}, \ (\mathfrak{p})$$
$$\vdots$$
$$\varrho_\nu \equiv \pi^{e_\nu}, \ (\mathfrak{p}),$$

wo $e_1, e_2, \ldots e_\nu$ mit den Zahlen $1, 2, \ldots n(\mathfrak{p}) - 1$, abgesehen von der Reihenfolge, übereinstimmen. Also ist

$$\varrho_1 \cdot \varrho_2 \ldots \varrho_\nu \equiv \pi^{\frac{n(\mathfrak{p})-1}{2} n(\mathfrak{p})}, \ (\mathfrak{p}).$$

Weil nun π Primitivzahl ist, so ist

$$\pi^{\frac{n(\mathfrak{p})-1}{2}} \equiv -1, (\mathfrak{p}),$$

und da ferner $n(\mathfrak{p})$ ungerade ist, erhält man schließlich:

$$\varrho_1 \cdot \varrho_2 \ldots \varrho_\nu \equiv -1, (\mathfrak{p}).$$

Aus dem Satz von Wilson läßt sich eine Bedingung ableiten für die Lösbarkeit der Kongruenz:

$$\xi^2 \equiv -1, (\mathfrak{p}),$$

worin $\mathfrak{p}$ zu (2) prim ist, oder man kann die Moduln $\mathfrak{p}$ näher bezeichnen, für welche diese Kongruenz durch eine ganze Zahl des Körpers lösbar ist. Wir gehen auf diese Frage näher ein.

Die Kongruenz $\xi^2 \equiv -1, (\mathfrak{p})$ ist offenbar stets lösbar im Körper $k(\sqrt{-1})$, und von diesem Körper sei daher im folgenden abgesehen.

$\mathfrak{p}$ möge zunächst ein Primideal ersten Grades bezeichnen, so sind die Zahlen

$$1, 2, \ldots p-1,$$

oder

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots -2, -1, 1, 2, \ldots \frac{p-3}{2}, \frac{p-1}{2},$$

ein volles System inkongruenter Zahlen. Dann ist

$$\varrho_1 \cdot \varrho_2 \ldots \varrho_\nu = (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}\right)^2 = (-1)^{\frac{p-1}{2}} \mu^2$$

und folglich

$$(-1)^{\frac{p-1}{2}} \mu^2 \equiv -1, (\mathfrak{p}).$$

Es stellt daher die Zahl μ eine Lösung der Kongruenz $\xi^2 \equiv -1, (\mathfrak{p})$ dann und nur dann vor, wenn die durch $\mathfrak{p}$ teilbare rationale Primzahl p der Bedingung $p \equiv 1, (4)$ genügt.

Falls $\mathfrak{p}$ aber ein Primideal 2ten Grades ist, so stellen nun die Zahlen $r + s\omega$ für

$$r, s = -\frac{p-1}{2}, -\frac{p-3}{2}, \ldots -2, -1, 1, 2, \ldots \frac{p-1}{2},$$

zusammen mit den Zahlen

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots -1, 1, \ldots \frac{p-1}{2}$$

und

$$-\frac{p-1}{2}\omega, \ldots \frac{p-1}{2}\omega$$

ein vollständiges System inkongruenter Zahlen dar, und es ist:

$$\varrho_1 \cdot \varrho_2 \ldots \varrho_\nu = (-1)^{\frac{(p-1)^2}{2} + p - 1} \left(1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}\right)^4 \omega^{p-1} \cdot \Pi (r_1 + s_1 \omega)^2,$$

wobei das Produkt $\prod$ genommen ist für alle Kombinationen von r_1 von 1 bis $\frac{p-1}{2}$ und von s_1 von $-\frac{p-1}{2}$ bis $+\frac{p-1}{2}$. Weil p ungerade ist, so ist $\frac{(p-1)^2}{2}+p-1=(p-1)\left(1+\frac{p-1}{2}\right)$ gerade, also die rechte Seite der letzten Gleichung das positive Quadrat einer ganzen Zahl des Körpers:

$$\varrho_1\varrho_2\ldots\varrho_\nu=\mu^2$$

und

$$\varrho_1\varrho_2\ldots\varrho_\nu=\mu^2\equiv-1,\ (\mathfrak{p}).$$

Die Kongruenz

$$\xi^2\equiv-1,\ (\mathfrak{p})$$

ist somit in einem beliebigen Körper stets lösbar für einen Primmodul $\mathfrak{p}$ zweiten Grades.

20. Lineare Kongruenzen nach Idealen.

Ein besonders wichtiger Fall der Kongruenzen mit unbestimmten Größen ist die Kongruenz ersten Grades oder die *lineare* Kongruenz:

$$\alpha\xi\equiv\beta,\ (\mathfrak{j}).$$

Die wichtigste Frage, welche für eine solche Kongruenz zuerst zu entscheiden ist, lautet nun: *Unter welcher Bedingung ist eine lineare Kongruenz durch eine ganze Zahl des Körpers lösbar?*

1. Annahme. Das Ideal (α) und das Ideal $\mathfrak{j}$ seien prim zueinander. Wenn alsdann statt ξ alle Zahlen ϱ eines vollständigen Restsystems nach $\mathfrak{j}$ gesetzt werden:

$$\alpha\varrho_1,\ \alpha\varrho_2,\ \ldots\ \alpha\varrho_\nu,$$

so müssen diese Zahlen wieder ein vollständiges Restsystem bilden. Wäre nämlich etwa

$$\alpha\varrho_s\equiv\alpha\varrho_{s'},\ (\mathfrak{j})$$

oder

$$\alpha(\varrho_s-\varrho_{s'})\equiv0,\ (\mathfrak{j}),$$

so müßte

$$\varrho_s-\varrho_{s'}\equiv0,\ (\mathfrak{j})$$

sein, weil α nach Voraussetzung prim ist zu $\mathfrak{j}$, und dies widerspricht der Definition der Zahlen ϱ. Die Zahl β muß daher einer und kann *nur einer* der Zahlen $\alpha\varrho$ kongruent sein; wenn

$$\alpha\varrho\equiv\beta,\ (\mathfrak{j})$$

ist, so ist $\xi=\varrho$ eine Lösung der linearen Kongruenz, und zwar die einzig mögliche aus dem ganzen Restsystem. Außer dieser genügt

aber jede Zahl $\varrho + gi + f(i_1 + i_2\omega)$ derselben Kongruenz, wenn i und $i_1 + i_2\omega$ Normalbasiszahlen des Ideals $\mathfrak{j}$ bezeichnen.

Mit Benützung des Fermatschen Satzes kann man ϱ noch näher angeben. Es ist ja, nach der Voraussetzung über α und $\mathfrak{j}$:

$$\alpha^{\Phi(\mathfrak{j})} \equiv 1,\ (\mathfrak{j}),$$

daher wird

$$\xi \equiv \alpha^{\Phi(\mathfrak{j})-1} \cdot \beta,\ (\mathfrak{j}),$$

oder man kann

$$\varrho = \beta\alpha^{\Phi(\mathfrak{j})-1}$$

setzen.

Insbesondere gelten die bisherigen Resultate auch, wenn α und $\mathfrak{j}$ prim zueinander sind und β eine Einheit (vergl. Nr. 22, S. 98) des Körpers bedeutet.

Die Betrachtungen zur Lösung der speziellen linearen Kongruenzen stimmen überein mit den Betrachtungen für die Lösung von Kongruenzen mit rationalen ganzen Zahlen. Während aber hier die unbestimmte Gleichung

$$ax + by = 1$$

mit Hilfe einer Kettenbruchentwicklung gelöst werden kann, ist dies nicht mehr für die allgemeineren linearen Kongruenzen der Fall da ja selbst für Zahlen eines quadratischen Körpers nicht mehr das Euklidische Teilerverfahren allgemein gilt, auf dem im Grund jener Algorithmus beruht.

2. Annahme. Es möge nun der allgemeinere Fall vorliegen, daß (α) und $\mathfrak{j}$ den größten gemeinsamen (Ideal-) Teiler $\mathfrak{d}$ besitzen. Dann kann die Kongruenz

$$\alpha\xi \equiv \beta,\ (\mathfrak{j})$$

aber offenbar nur lösbar sein, wenn der Teiler $\mathfrak{d}$ auch in (β) aufgeht. Denn wenn die Gleichung gilt:

$$(\alpha\xi - \beta) = \mathfrak{t}\mathfrak{j} = \mathfrak{t}\mathfrak{j}^*\mathfrak{d},$$

so ist

$$\alpha\xi - \beta \equiv -\beta \equiv 0,\ (\mathfrak{d}).$$

Ist aber die Bedingung $\beta \equiv 0,\ (\mathfrak{d})$ erfüllt, so ist die Kongruenz auch lösbar.

In der Tat, schreibt man etwa $\mathfrak{j} = \mathfrak{j}^*\mathfrak{d}$, ferner $(\alpha) = \mathfrak{a}\mathfrak{d}$ und $(\beta) = \mathfrak{b}\mathfrak{d}$, wo nun nach Voraussetzung $\mathfrak{a}$ und $\mathfrak{j}^*$ prim zueinander sind, so kann man stets eine ganze Zahl δ des Körpers von der Beschaffenheit angeben, daß (δ) durch die erste, aber keine höhere Potenz von $\mathfrak{d}$ teilbar ist und $\frac{(\delta)}{\mathfrak{d}} = \mathfrak{d}_1$ prim ist zu $\mathfrak{j}$ (die Richtigkeit dieser Be-

hauptung wird in der analytischen Zahlentheorie streng bewiesen), indem man das Ideal $\mathfrak{d}_1$ diesen Bedingungen entsprechend wählen kann. Ferner bestimme man aus dem Ideal $\mathfrak{d}_1$ eine Zahl λ, die prim ist zu $\mathfrak{j}$, was ja nach der Bestimmung von $\mathfrak{d}_1$ möglich sein muß, und setze nun:

$$\alpha_1 = \frac{\alpha\lambda}{\delta}, \quad \beta_1 = \frac{\beta\lambda}{\delta}.$$

Alsdann sind die Zahlen α_1, β_1 ganze Zahlen des Körpers, und wenn die Kongruenz $\alpha\xi \equiv \beta$, $(\mathfrak{j})$ durch eine ganze Zahl des Körpers $\xi = \varrho$ lösbar ist, so ist auch die Kongruenz $\alpha_1\xi \equiv \beta_1$, $(\mathfrak{j}^*)$ durch dieselbe Zahl befriedigt, *und umgekehrt.*

Wenn nämlich zuerst die Kongruenz gilt:

$$\alpha\varrho \equiv \beta, \ (\mathfrak{j}),$$

so ist nach der Bestimmung von λ und δ auch:

$$\lambda\alpha\varrho \equiv \lambda\beta, \ (\mathfrak{j}),$$

oder

$$\delta\alpha_1\varrho \equiv \delta\beta_1, \ (\mathfrak{j}),$$

folglich

$$\alpha_1\varrho \equiv \beta_1, \ (\mathfrak{j}^*).$$

Umgekehrt, wenn $\alpha_1\varrho \equiv \beta_1$, $(\mathfrak{j}^*)$ gilt, so ist auch $\delta\alpha_1\varrho \equiv \delta\beta_1$, $(\mathfrak{j})$, oder $\lambda\alpha\varrho \equiv \lambda\beta$, $(\mathfrak{j})$ und weil (λ) prim ist zu $\mathfrak{j}$, schließlich:

$$\alpha\varrho \equiv \beta, \ (\mathfrak{j}).$$

Nun ist ja aber α_1 prim zu $\mathfrak{j}^*$, also ist die Kongruenz

$$\alpha_1\xi - \beta_1 \equiv 0, \ (\mathfrak{j}^*)$$

wirklich durch eine ganze Zahl $\xi = \varrho$ erfüllbar, und es hat auch die gegebene Kongruenz

$$\alpha\xi \equiv \beta, \ (\mathfrak{j})$$

die Zahl ϱ als Lösung, wenn der größte gemeinsame Teiler von (α) und $\mathfrak{j}$ in (β) aufgeht.

Man kann ϱ stets als eine Zahl wählen aus dem einfachsten vollständigen Restsystem nach $\mathfrak{j}^*$, dann sind *alle* Lösungen der ursprünglichen Kongruenz in der Formel inbegriffen:

$$\xi = \varrho + g i^* + f(i_1^* + i_2^*\omega),$$

wo i^*, $i_1^* + i_2^*\omega$ die Basiszahlen des Ideals $\mathfrak{j}^*$ und g, f rationale ganze positive oder negative Zahlen bedeuten. Setzt man analog $\mathfrak{j} = (i, i_1 + i_2\omega)$, so befinden sich unter den Zahlen ξ offenbar $\frac{i\,i_2}{i^*\,i_2^*}$ oder $n(\mathfrak{d})$ nach dem Modul $\mathfrak{j}$ inkongruente Zahlen, und man kann daher den zusammenfassenden Satz formulieren:

Satz. *Eine lineare Kongruenz:*

$$\alpha\xi \equiv \beta, \ (\mathfrak{j})$$

ist dann und nur dann durch eine ganze Zahl des Körpers lösbar, wenn der größte gemeinsame Teiler $\mathfrak{d}$ *des Ideals* (α) *und des Ideals* $\mathfrak{j}$ *auch Teiler des Ideals* (β) *ist, und zwar besitzt die Kongruenz alsdann genau* $n(\mathfrak{d})$ *inkongruente Lösungen.*

Dieser Satz gilt seiner ganzen Entwicklung nach auch dann, wenn der Modul $\mathfrak{j}$ eine ganze Zahl γ des Körpers bezeichnet, und zwar kann dann das Resultat auch so formuliert werden: Eine Diophantische Gleichung mit ganzen, dem Körper $k(\sqrt{m})$ angehörenden Koeffizienten α, β, γ:

$$\alpha\xi + \gamma\eta = \beta$$

besitzt dann und nur dann (unendlich viele) Lösungen, wenn der größte gemeinsame Idealteiler von (α) und (γ) auch in (β) aufgeht.

Für manche Zwecke ist auch ein Satz über simultane Kongruenzen brauchbar, dessen einfachster Fall folgendermaßen ausgesprochen werden kann:

Satz. *Wenn* $\mathfrak{a}_1, \mathfrak{a}_2$ *zwei Ideale bezeichnen, die prim zueinander sind, und wenn* α_1, α_2 *irgend welche ganze Zahlen des Körpers sind, so gibt es stets eine ganze Zahl* ξ *des Körpers, für welche gleichzeitig die Kongruenzen gelten:*

$$\xi \equiv \alpha_1, \ (\mathfrak{a}_1), \quad \xi \equiv \alpha_2, \ (\mathfrak{a}_2).$$

Beweis. Die ganze Zahl ϱ des Körpers genüge der Kongruenz

$$\xi \equiv \alpha_1, \ (\mathfrak{a}_1),$$

und es sei $\mathfrak{a}_1 = (a, a_1 + a_2\omega)$, dann sind alle Lösungen dieser Kongruenz in der linearen Form

$$\xi = \varrho + \sigma a + \tau(a_1 + a_2\omega)$$

enthalten, wo σ und τ ganze Zahlen des Körpers sind. Damit ξ auch der zweiten Kongruenz genügt, hat man σ, τ noch so zu wählen, daß

$$\varrho + \sigma a + \tau(a_1 + a_2\omega) \equiv \alpha_2, \ (\mathfrak{a}_2)$$

oder

$$\sigma a + \tau(a_1 + a_2\omega) \equiv \alpha_2 - \varrho, \ (\mathfrak{a}_2)$$

ausfällt. Man setze nun

$$\sigma = A\xi_1, \quad \tau = B\xi_1,$$

und wähle A, B als ganze rationale Zahlen derart, daß

$$Aa + B(a_1 + a_2\omega) = \alpha_1^*$$

prim zu $\mathfrak{a}_2$ wird, was stets möglich ist, da α_1^* eine Zahl aus $\mathfrak{a}_1$ ist und

$\mathfrak{a}_1$, $\mathfrak{a}_2$ prim zueinander sein sollen. Alsdann ist aber ξ_1 bestimmbar, so daß die Kongruenz

$$\alpha_1^* \xi_1 \equiv \alpha_2 - \varrho,\ (\mathfrak{a}_2)$$

erfüllt ist, und nun ergeben σ, τ den gesuchten Wert für ξ.

Auf die Form

$$\xi \equiv \alpha_1,\ (\mathfrak{a}_1), \quad \xi \equiv \alpha_2,\ (\mathfrak{a}_2)$$

läßt sich auch das (scheinbar allgemeinere) simultane System

$$\varkappa_1 \xi \equiv \alpha_1,\ (\mathfrak{a}_1), \quad \varkappa_2 \xi \equiv \alpha_2,\ (\mathfrak{a}_2)$$

zurückführen. Falls $\varkappa_1$ prim zu $\mathfrak{a}_1$ und $\varkappa_2$ prim zu $\mathfrak{a}_2$ ist, braucht man dazu nur die Kongruenzen mit $\varkappa_1^{\Phi(\mathfrak{a}_1)-1}$ resp. mit $\varkappa_2^{\Phi(\mathfrak{a}_2)-1}$ zu multiplizieren. Leicht ergeben sich auch die notwendigen und hinreichenden Bedingungen für die Lösbarkeit der simultanen Kongruenzen, wenn $\varkappa_1$ und $\mathfrak{a}_1$ einerseits und $\varkappa_2$ und $\mathfrak{a}_2$ andererseits nicht mehr prim zueinander sein sollten.

Als fernere Anwendung des Satzes über die Primitivzahlen soll schließlich noch ein Kriterium für die Lösbarkeit einer Kongruenz zweiten Grades entwickelt werden.

21. Quadratische Kongruenzen und das Symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$.

Die allgemeinste Kongruenz 2ten Grades nach dem Modul $\mathfrak{p}$ ist von der Form:

$$\alpha\xi^2 + 2\alpha_1\xi + \alpha_2 \equiv 0,\ (\mathfrak{p}), \tag{1}$$

in der die drei Koeffizienten α, α_1, α_2 beliebige ganze Zahlen des Körpers sind. Wenn α, α_1, α_2 zu $\mathfrak{p}$ prim sind, so besitzt eine solche Kongruenz eine Wurzel, falls die Kongruenz

$$\alpha(\alpha\xi^2 + 2\alpha_1\xi + \alpha_2) \equiv 0,\ (\mathfrak{p})$$

lösbar ist, und umgekehrt. Nun kann man aber diese letzte Kongruenz schreiben:

$$(\alpha\xi + \alpha_1)^2 + \alpha\alpha_2 - \alpha_1^2 \equiv 0,\ (\mathfrak{p}),$$

und die Frage, ob die Kongruenz (1) in ganzen Zahlen des Körpers $k(\sqrt{m})$ lösbar ist, ist identisch mit der Frage, ob die miteinander verknüpften Kongruenzen

$$\sigma^2 + \alpha^* \equiv 0,\ (\mathfrak{p}) \tag{2a}$$

und

$$\alpha\xi + \alpha_1 \equiv \sigma,\ (\mathfrak{p}) \tag{2b}$$

lösbar sind. Die letztere lineare Kongruenz läßt sich stets befriedigen, wenn σ bekannt ist, es bleibt also nur die Lösbarkeit der Kongruenz (2a) zu entscheiden.

Ist α oder α_2 durch $\mathfrak{p}$ teilbar, so reduziert sich die Kongruenz (1) auf eine Kongruenz ersten Grades. Wenn andererseits α_1 durch $\mathfrak{p}$ teilbar ist, so reduziert sich die allgemeine Kongruenz auf:

$$\alpha\xi^2 + \alpha_2 \equiv 0,\ (\mathfrak{p}), \tag{3}$$

und diese Kongruenz ist dann, und sicher dann lösbar, wenn

$$\alpha^{n(\mathfrak{p})-2}(\alpha\xi^2 + \alpha_2) \equiv 0,\ (\mathfrak{p}) \tag{4}$$

lösbar ist, da α und folglich auch $\alpha^{n(\mathfrak{p})-2}$ zu $\mathfrak{p}$ prim sind. Wegen des Satzes von Fermat für Ideale kann aber statt der Kongruenz (4) auch geschrieben werden:

$$\xi^2 + \alpha^* \equiv 0,\ (\mathfrak{p}),$$

und die Frage nach der Lösbarkeit einer Kongruenz zweiten Grades kommt daher immer zurück entweder auf die Frage nach der Lösbarkeit einer Kongruenz ersten Grades im speziellen Fall, oder einer reinen Kongruenz zweiten Grades von der Form:

$$\xi^2 - \alpha \equiv 0,\ (\mathfrak{p}).$$

Es braucht daher nur diese Kongruenz untersucht zu werden und wir beginnen mit dem Fall, daß der Primmodul $\mathfrak{p}$ nicht aufgeht im Ideal (2).

Die Kongruenz ist durch $\xi \equiv 0$ lösbar und besitzt überhaupt nur *eine* doppelt zählende Lösung, wenn $\alpha \equiv 0,\ (\mathfrak{p})$ ist, somit bleibt nur der Fall übrig, daß (α) prim ist zu $\mathfrak{p}$.

Ist nun π eine Primitivzahl nach $\mathfrak{p}$, so gibt es einen ganzzahligen positiven Exponenten a von der Eigenschaft, daß

$$\alpha \equiv \pi^a,\ (\mathfrak{p})$$

ist. Aus diesem Ansatz ersieht man, daß die gegebene Kongruenz dann lösbar sein muß, wenn a eine *gerade* Zahl ist, und hierfür ist die notwendige und hinreichende Bedingung, daß

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv (\pi^a)^{\frac{n(\mathfrak{p})-1}{2}} \equiv +1,\ (\mathfrak{p})$$

ausfällt, wie nun gezeigt werden soll.

Satz. *Die quadratische Kongruenz* $\xi^2 \equiv \alpha,\ (\mathfrak{p})$, *nach einem Primmodul* $\mathfrak{p}$, *welcher nicht in 2 aufgeht, ist für ein* α, *das prim ist zu* $\mathfrak{p}$, *dann und nur dann durch zwei inkongruente ganze Zahlen des Körpers* $k(\sqrt{m})$ *lösbar, wenn*

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv +1,\ (\mathfrak{p})$$

ausfällt.

Wenn eine Kongruenz $\xi^2 \equiv \alpha,\ (\mathfrak{p})$ unter der Voraussetzung, daß $\mathfrak{p}$ nicht in α aufgeht, lösbar ist, so sagt man auch, α ist *quadratischer*

Rest nach $\mathfrak{p}$, im entgegengesetzten Fall heißt α *quadratischer Nichtrest nach* $\mathfrak{p}$. Im ersten Fall soll gesetzt werden

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1,$$

im zweiten Fall

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1.$$

Nach dem verallgemeinerten Satze von Fermat gilt nun für eine durch $\mathfrak{p}$ nicht teilbare Zahl α:

$$\alpha^{n(\mathfrak{p})-1} \equiv 1, \ (\mathfrak{p})$$

oder

$$\alpha^{n(\mathfrak{p})-1} - 1 \equiv 0, \ (\mathfrak{p}).$$

Zerlegt man die linke Seite dieser Kongruenz in die beiden Faktoren $\alpha^{\frac{n(\mathfrak{p})-1}{2}} + 1$ und $\alpha^{\frac{n(\mathfrak{p})-1}{2}} - 1$ und berücksichtigt, daß ein gemeinsamer Idealteiler dieser beiden Faktoren auch in $2\alpha^{\frac{n(\mathfrak{p})-1}{2}}$ und somit in 2 aufgehen müßte, so folgt, daß für einen in 2 nicht aufgehenden Modul $\mathfrak{p}$ eine und nur eine der beiden Kongruenzen:

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv 1, \ (\mathfrak{p})$$

oder

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv -1, \ (\mathfrak{p})$$

erfüllt sein kann.

Falls die erste dieser Kongruenzen erfüllt ist, so gilt unter Benutzung des Ausdrucks $\alpha \equiv \pi^a$, $(\mathfrak{p})$:

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv (\pi^a)^{\frac{n(\mathfrak{p})-1}{2}} \equiv 1, (\mathfrak{p}),$$

es muß a gerade sein, und es ist $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$. Falls aber die zweite Kongruenz erfüllt ist, so ist:

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv (\pi^a)^{\frac{n(\mathfrak{p})-1}{2}} \equiv -1, \ (\mathfrak{p}),$$

also a sicher ungerade, und daher $\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$.

Wir haben damit eine notwendige Ergänzung des Satzes und man kann also sagen:

Ist $\mathfrak{p}$ ein nicht in 2 aufgehendes Primideal und α eine durch $\mathfrak{p}$ nicht teilbare ganze Zahl des Körpers $k(\sqrt{m})$, so ist α quadratischer Rest oder Nichtrest nach $\mathfrak{p}$, je nachdem

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \pm 1, \ (\mathfrak{p})$$

ist. Oder es gilt stets die Kongruenz

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right), \ (\mathfrak{p}),$$

in welcher die Einzelfälle zusammengefaßt sind.

Aus dem Satz über die Existenz von Primitivzahlen nach $\mathfrak{p}$ und der Tatsache, daß die $n(\mathfrak{p}) - 1$ Potenzen $\pi, \pi^2, \ldots$ einer Primitivzahl ein volles Restsystem inkongruenter Zahlen nach $\mathfrak{p}$ darstellen, folgt die weitere Behauptung:

Satz. *Nach einem nicht in* (2) *aufgehenden Primideal* $\mathfrak{p}$ *gibt es* $\frac{n(\mathfrak{p})-1}{2}$ *inkongruente quadratische Reste und gleichviele Nichtreste.*

Satz. *Sind* α *und* β *zwei durch das Primideal* $\mathfrak{p}$ *nicht teilbare ganze Zahlen des Körpers* $k(\sqrt{m})$, *so ist:*

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right).$$

Beweis. Es ist

$$\left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{\frac{n(\mathfrak{p})-1}{2}}, \quad \left(\frac{\beta}{\mathfrak{p}}\right) \equiv \beta^{\frac{n(\mathfrak{p})-1}{2}}, \ (\mathfrak{p}),$$

also

$$\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) \equiv (\alpha\beta)^{\frac{n(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha\beta}{\mathfrak{p}}\right), \ (\mathfrak{p}),$$

daher folgt:

$$\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha\beta}{\mathfrak{p}}\right),$$

wie es der Satz behauptet.

Der bisher ausgeschlossene Fall, daß $\mathfrak{p}$ ein in 2 aufgehendes Primideal ist, erledigt sich leicht direkt.

Zerfällt nämlich im Körper $k(\sqrt{m})$ das Ideal (2) in $\mathfrak{p} \cdot \mathfrak{p}'$, so ist $n(\mathfrak{p}) = 2$, $\Phi(\mathfrak{p}) = 1$, und da α prim zu (2) ist, so ist es auch quadratischer Rest nach $\mathfrak{p}$, weil alsdann stets

$$\alpha \equiv 1, \ (\mathfrak{p})$$

ist. Falls aber (2) selbst Primideal ist, nämlich für den Fall $m \equiv 5, (8)$, so sind die nach $\mathfrak{p} = (2)$ inkongruenten Zahlen des Körpers: $1, \omega, 1 + \omega$, und es ist α wiederum stets quadratischer Rest nach $\mathfrak{p}$, weil die quadratische Kongruenz für $\alpha \equiv 1, \omega, 1 + \omega$ lösbar ist, wie man durch direkte Berechnung der Wurzeln erkennt.

Das Symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$, welches also für ein in 2 nicht aufgehendes

Primideal $\mathfrak{p}$, und wenn α prim zu $\mathfrak{p}$ ist, nur der beiden Werte $+1$ oder -1 fähig ist, je nach dem Restcharakter von α nach $\mathfrak{p}$, soll auch jetzt wieder das Legendresche Symbol heißen, weil es nur die Erweiterung des früher eingeführten Symbols auf Ideale und algebraische Zahlen ist.

Sucht man nun die bisherigen Betrachtungen zu erweitern, indem man eine quadratische Kongruenz

$$\xi^2 - \alpha \equiv 0, \; (\mathfrak{a})$$

nach einem beliebigen Modul $\mathfrak{a}$ zugrunde legt, so stößt man zunächst auf die Frage, die hier allein behandelt werden soll: unter welcher Bedingung ist eine quadratische Kongruenz

$$\xi^2 - \alpha \equiv 0, \; (\mathfrak{p}^k)$$

nach der k^{ten} Potenz eines Primideals $\mathfrak{p}$ lösbar, wenn α prim ist zu $\mathfrak{p}$?

Es sind wieder zwei Fälle zu unterscheiden: 1.) $\mathfrak{p}$ ist prim zur Zahl 2 und 2.) $\mathfrak{p}$ geht in der Zahl 2 auf.

Im ersten Fall sieht man sofort ein, daß die Kongruenz jedenfalls nur dann lösbar sein kann, wenn schon die Kongruenz

$$\xi^2 - \alpha \equiv 0, \; (\mathfrak{p})$$

eine Lösung besitzt, also wenn $\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$ ist.

Ist aber diese Bedingung erfüllt, und bezeichnet λ eine beliebige Lösung dieser letzteren Kongruenz, wobei also λ ebenfalls prim ist zu $\mathfrak{p}$, so sind unendlich viele Lösungen der Kongruenz in der Form:

$$\xi = \lambda + p\varrho$$

enthalten, wenn ϱ alle Zahlen des Körpers durchläuft. Unter den Zahlen $\lambda + p\varrho$ muß aber wiederum eine Wurzel der Kongruenz

$$\xi^2 - \alpha \equiv 0, \; (\mathfrak{p}^k),$$

falls eine solche existiert, vorhanden sein.

Wir setzen nun zunächst $k = 2$ und nehmen an, daß p nicht durch $\mathfrak{p}^2$ teilbar ist, dann hat man noch den Wert ϱ derart zu bestimmen, daß

$$(\lambda + p\varrho)^2 - \alpha \equiv 0, \; (\mathfrak{p}^2)$$

wird. Da $p^2 \equiv 0, \; (\mathfrak{p}^2)$ ist, so muß danach ϱ der Kongruenz

$$2p\lambda\varrho + \lambda^2 - \alpha \equiv 0, \; (\mathfrak{p}^2)$$

entsprechend bestimmt werden.

Wäre nun $\lambda^2 - \alpha$ selbst durch $\mathfrak{p}^2$ teilbar, so brauchte man nur $\varrho \equiv 0, \; (\mathfrak{p})$ zu setzen, um eine Lösung der Kongruenz zu haben.

Wird dieser Fall ausgeschlossen, so ist nun zu entscheiden, ob ϱ als ganze Zahl des Körpers so gewählt werden kann, daß die lineare

Kongruenz $2p\lambda\varrho + \lambda^2 - \alpha \equiv 0$, $(\mathfrak{p}^2)$ erfüllt ist. Aus dem allgemeinen Satz über die Lösung linearer Kongruenzen folgt aber, daß dies der Fall ist, wenn der größte gemeinsame Faktor von $2p\lambda$ und $\mathfrak{p}^2$, in unserm Fall also das Primideal $\mathfrak{p}$ in $\lambda^2 - \alpha$ ebenfalls als Faktor enthalten ist, was ja zutrifft.

Ist nun ϱ der letzten linearen Kongruenz entsprechend bestimmt, so stellt der Ausdruck $\xi = \lambda + p\varrho$ jetzt eine Lösung der Kongruenz

$$\xi^2 - \alpha \equiv 0, \ (\mathfrak{p}^2)$$

dar. Man sieht leicht, daß man durch ganz analoge Schlüsse wieder zeigen kann, daß dann auch die Kongruenz

$$\xi^2 \equiv \alpha, \ (\mathfrak{p}^3)$$

eine Lösung besitzt, und erhält schließlich nach weiterer Verallgemeinerung den Satz:

Satz. *Ist $\mathfrak{p}$ ein zu (2) relativ primes Primideal des Körpers $k(\sqrt{m})$, das nicht in der Diskriminante des Körpers aufgeht, und ist α eine durch $\mathfrak{p}$ nicht teilbare ganze Zahl des Körpers, so besitzt eine Kongruenz*

$$\xi^2 \equiv \alpha, \ (\mathfrak{p}^k)$$

Lösungen oder nicht, je nachdem $\left(\frac{\alpha}{p}\right) = +1$ oder $\left(\frac{\alpha}{p}\right) = -1$ ausfällt.

Wenn $\mathfrak{p}^2$ in der rationalen Primzahl p aufgeht, d. h. wenn p ein Teiler der Diskriminante ist, so müssen die Untersuchungen nach der Lösbarkeit der allgemeinen Kongruenz etwas modifiziert werden. Es ist leicht einzusehen, daß dann die Kongruenz

$$\xi^2 - \alpha \equiv 0, \ (\mathfrak{p}^k)$$

für einen beliebigen Exponenten k stets und nur lösbar ist, wenn auch die Kongruenz

$$\xi^2 - \alpha \equiv 0, \ (\mathfrak{p}^2)$$

Lösungen besitzt.

Der bisher ausgeschlossene Fall, daß $\mathfrak{p}$ in der Zahl 2 aufgeht, läßt sich in ganz ähnlicher Weise wie der vorige Fall erledigen und liefert folgenden Satz:

Satz. *Ist $\mathfrak{p}$ ein in 2 aufgehendes Primideal des Körpers $k(\sqrt{m})$ und ist α eine zu $\mathfrak{p}$ relativ prime ganze Zahl des Körpers, so hat die Kongruenz*

$$\xi^2 - \alpha \equiv 0, \ (\mathfrak{p}^k)$$

dann und nur dann für jeden Exponenten k eine Lösung, wenn

$$\xi^2 - \alpha \equiv 0, \ (\mathfrak{p}^6) \tag{I}$$

eine Lösung besitzt, falls $\mathfrak{p}$ ein Primideal ersten Grades ist, und wenn zweitens

$$\xi^2 - \alpha \equiv 0, \ (\mathfrak{p}^5) \tag{II}$$

eine Lösung besitzt, falls $\mathfrak{p}$ ein Primideal zweiten Grades ist.

Auch die Frage, für welche Werte von α die Kongruenzen (I) resp. (II) lösbar sind, läßt sich leicht durch eine Diskussion aller möglichen einzelnen Fälle entscheiden; man findet, daß für die beiden Fälle $\alpha \equiv 1, (\mathfrak{p}^6)$ resp. $\alpha \equiv 1, (8)$ sein muß. Beidemal erhält man vier inkongruente Lösungen ± 1 und ± 3.

Wenn auch an dieser Stelle noch die Mittel zur Berechnung des Symbols $\left(\frac{d}{p}\right)$ fehlen, so kann dem Leser doch nicht dringend genug empfohlen werden, alle bisher entwickelten Begriffe und Sätze sich dadurch ganz klar zu machen, daß er spezielle Körper: $k(\sqrt{-1})$, $k(\sqrt{-2})$, $k(\sqrt{2})$ usw. nach den angegebenen Methoden ausführlich zahlenmäßig behandelt und von allen etwa möglichen Vereinfachungen der Theorie sich Rechenschaft gibt.

22. Einheiten des quadratischen Zahlkörpers.

Unter den ganzen Zahlen eines Zahlkörpers verdienen ein besonderes Interesse die „*Einheiten*" des Körpers. Man versteht darunter jede ganze Zahl des Körpers, welche in ± 1 aufgeht oder, was dasselbe aussagt, jede ganze Zahl, deren Norm gleich ± 1 ist.

Die Aufgabe, welche sich im Anschluß an diese Definition sofort aufdrängt, besteht darin, die eventuelle *Existenz* solcher von ± 1 verschiedenen Einheiten nachzuweisen, und dies gelingt sehr leicht auf Grund des Minkowskischen Satzes, wie nun gezeigt werden soll.

1. Satz. *In einem beliebigen imaginären Zahlkörper sind* ± 1 *die einzigen Einheiten, außerdem existieren in dem Körper* $k(\sqrt{-1})$ *als weitere Einheiten noch* $\pm\sqrt{-1}$ *und in dem Körper* $k(\sqrt{-3})$ *die Einheiten* $\pm \frac{1 \pm \sqrt{-3}}{2}$.

Beweis. Betrachten wir zuerst den Körper $k(\sqrt{-1})$, so ist in diesem eine ganze Zahl $x + \sqrt{-1}\, y$ dann eine Einheit, wenn ihre Norm gleich ± 1 ist, d. h. wenn die Gleichung besteht:

$$n(x + \sqrt{-1}\, y) = x^2 + y^2 = \pm 1.$$

Die Gleichung

$$x^2 + y^2 = -1$$

ist offenbar für kein reelles x und kein reelles y zu befriedigen, dagegen ist die Gleichung

$$x^2 + y^2 = 1$$

befriedigt für jedes der 4 Wertesysteme

$$\begin{aligned}
&1. \quad x = 1, \quad && y = 0\\
&2. \quad x = -1, \quad && y = 0\\
&3. \quad x = 0, \quad && y = 1\\
&4. \quad x = 0, \quad && y = -1
\end{aligned}$$

und offenbar *nur* für diese. Es sind also

$$+1, \quad -1, \quad +\sqrt{-1}, \quad -\sqrt{-1}$$

die einzigen Einheiten des Körpers. Sie sind die Quadratwurzeln aus ± 1, und man pflegt darum diese Einheiten als Einheitswurzeln zu bezeichnen.

Ferner ist im Körper $k(\sqrt{-3})$ eine ganze Zahl

$$x + \frac{1+\sqrt{-3}}{2} y$$

dann eine Einheit des Körpers, wenn wieder:

$$n\left(x + \frac{1+\sqrt{-3}}{2} y\right) = (x + \tfrac{1}{2} y)^2 + \tfrac{3}{4} y^2 = \pm 1$$

ist, wo aber ähnlich wie vorhin nur die Gleichung in Betracht kommen kann:

$$(x + \tfrac{1}{2} y)^2 + \tfrac{3}{4} y^2 = +1,$$

oder

$$x^2 + xy + y^2 = +1.$$

Diese Gleichung kann nur durch die folgenden Wertesysteme befriedigt werden:

$$\begin{aligned}
&1. \quad x = 1, \quad && y = 0\\
&2. \quad x = -1, \quad && y = 0\\
&3. \quad x = 1, \quad && y = -1\\
&4. \quad x = -1, \quad && y = 1\\
&5. \quad x = 0, \quad && y = 1\\
&6. \quad x = 0, \quad && y = -1,
\end{aligned}$$

diese Wertesysteme ergeben alsdann die folgenden Zahlen des Körpers $k(\sqrt{-3})$ als Einheiten:

$$\pm 1, \quad \pm \omega = \pm \frac{1+\sqrt{-3}}{2}, \quad \pm \omega' = \pm \frac{1-\sqrt{-3}}{2};$$

alle diese Zahlen sind dritte Einheitswurzeln.

Für jeden andern beliebigen imaginären Körper $k(\sqrt{m})$ ist eine ganze Zahl von der Form

$$x + \sqrt{m}\, y, \quad \text{falls } m \not\equiv 1, \ (4),$$

oder

$$x + \frac{1+\sqrt{m}}{2} y, \quad \text{falls } m \equiv 1, (4) \text{ ist,}$$

Einheit des Körpers, wenn x, y der Gleichung

$$x^2 - my^2 = \pm 1$$

resp.

$$(x + \frac{1}{2} y)^2 - \frac{m}{4} y^2 = \pm 1$$

genügen. Setzen wir $m = -|m|$, wo nun $|m|$ eine positive Zahl bedeutet, so müßten also x und y der Gleichung

$$x^2 + |m| y^2 = \pm 1$$

resp.

$$(x + \frac{1}{2} y)^2 + \frac{|m|}{4} y^2 = \pm 1$$

genügen.

Diese Gleichungen sind beide nur für das + Zeichen auf der rechten Seite lösbar, und da im ersten Fall $|m| \geqq 2$, im zweiten Fall $|m| \geqq 7$ zu nehmen ist, so ergeben sich als einzige Möglichkeiten für die Lösung:

$$x = +1, \quad y = 0,$$
$$x = -1, \quad y = 0,$$

denn für $|y| \geqq 1$ wird die linke Seite der Gleichung unter allen Umständen, d. h. für alle reellen x größer als 1. Es sind also ± 1 die einzigen Einheiten des allgemeinen imaginären Körpers.

2. Satz. *In jedem reellen Zahlkörper $k(\sqrt{m})$ existieren unendlich viele Einheiten verschieden von ± 1, und unter denselben gibt es eine Grundeinheit ε derart, daß $|\varepsilon| > 1$ ist und daß jede Einheit des Körpers sich in der Form $\pm \varepsilon^e$ darstellen läßt, wo e irgend einen positiven oder negativen ganzen rationalen Exponenten bedeutet.*

Der Beweis dieses Satzes zerlegt sich in zwei Teile: 1. in den Nachweis, daß in jedem Körper $k(\sqrt{m})$ Einheiten existieren, die von ± 1 verschieden sind; 2. in den Nachweis der Grundeinheit ε mit der im Satze bezeichneten Eigenschaft.

Der erste Teil dieses Beweises ist identisch mit dem Nachweis, daß die Gleichung

$$x^2 - my^2 = \pm 1, \quad (\text{wenn } m \not\equiv 1, (4)) \tag{1}$$

bezw.

$$(x + \frac{1}{2} y)^2 - \frac{m}{4} y^2 = \pm 1, \quad (\text{wenn } m \equiv 1, (4)) \tag{2}$$

wenigstens für das + Zeichen der rechten Seite durch rationale ganzzahlige Werte von x und y lösbar ist, für jedes ganzzahlige positive m.

d sei die Diskriminante des Körpers und ω, ω' bezeichnen wie immer die Zahlen $+\sqrt{m}$, falls $m \not\equiv 1$, (4) und $\frac{1+\sqrt{m}}{2}$, falls $m \equiv 1$, (4) ist. Dann sind:

$$f = x - \omega y \tag{3}$$

$$f' = x - \omega' y, \tag{4}$$

zwei lineare homogene Formen mit reellen Koeffizienten und der reellen positiven Determinante

$$\begin{vmatrix} 1 & -\omega \\ 1 & -\omega' \end{vmatrix} = \omega - \omega' = \sqrt{d},$$

ferner ist

$$ff' = x^2 - my^2, \quad \text{oder} \quad x^2 + xy + \frac{1-m}{4} y^2,$$

je nachdem $m \not\equiv 1$, (4) oder $m \equiv 1$, (4) vorausgesetzt wird.

Stellen $\varkappa$, $\varkappa_1$ irgend zwei beliebige positive reelle Zahlen vor, deren Produkt $\sqrt{d}$ ist, so lassen sich zwei ganze rationale Zahlen x, y, die nicht beide gleich Null sind, angeben, für welche

$$|f| = |x - \omega y| \leqq \varkappa \tag{5}$$

$$|f'| = |x - \omega' y| \leqq \varkappa_1 \tag{6}$$

ausfällt.

Man bestimme nun zwei ganzzahlige von Null verschiedene Werte x_1, y_1 so, daß für irgend eine positive Zahl $\varkappa$ und das entsprechende $\varkappa_1$, z. B. für $\varkappa = 1$, $\varkappa_1 = \sqrt{d}$,

$$|x_1 - \omega y_1| \leqq \varkappa, \quad |x_1 - \omega' y_1| \leqq \varkappa_1$$

wird und setze alsdann:

$$\alpha_1 = x_1 - \omega y_1.$$

Sodann bestimme man x_2, y_2 als rationale ganze Zahlen so, daß

$$|x_2 - \omega y_2| \leqq \left|\frac{\alpha_1}{2}\right|$$

$$|x_2 - \omega' y_2| \leqq \frac{2\sqrt{d}}{|\alpha_1|},$$

und setze

$$\alpha_2 = x_2 - \omega y_2,$$

so sind x_2, y_2 von x_1, y_1 und α_2 von α_1 verschieden. In der angefangenen Weise fahre man fort, bilde also eine Reihe von Zahlen

$$\alpha_1, \alpha_2, \alpha_3, \ldots \tag{7}$$

derart, daß

$$|\alpha_1| > |\alpha_2| > |\alpha_3| \ldots, \tag{8}$$

dann stellen die Ideale

$$(\alpha_1),\ (\alpha_2),\ (\alpha_3)\ \ldots$$

eine *unendliche* Anzahl von Idealen dar, deren Normen absolut genommen alle kleiner sind als $\sqrt{d}$. Es ist indessen früher bewiesen worden, daß es immer nur eine endliche Anzahl Ideale geben kann, deren Normen kleiner sind als eine endliche Zahl. Daher muß es in der unendlichen Reihe unendlich oft vorkommen, daß zwei Ideale einander gleich sind.

Ist nun etwa

$$(\alpha_1) = (\alpha_r),$$

so muß sowohl $\frac{\alpha_1}{\alpha_r}$ als auch $\frac{\alpha_r}{\alpha_1}$ eine ganze (*nicht rationale*) Zahl des Körpers, also

$$\alpha_1 = \varepsilon_r \alpha_r$$

sein, wo ε_r eine von ± 1 verschiedene *Einheit* ist. Da für die absoluten Beträge der Zahlen α die Ungleichung $|\alpha_1| > |\alpha_r|$ besteht, so muß notwendig $|\varepsilon_r| > 1$ sein.

In einem reellen Körper ist übrigens für eine ganze Zahl ε_r der absolute Betrag $|\varepsilon_r|$ nur gleich 1, wenn $\varepsilon_r = \pm 1$ ist. Denn ist allgemein $|\alpha| = |\alpha'|$ oder $|x + \omega y| = |x + \omega' y|$, dann muß notwendig $y = 0$ oder $\alpha = \pm \alpha'$ sein.

Mit diesem Schluß ist nun zugleich gezeigt, daß die Gleichung $x^2 - my^2 = 1$ resp. $x^2 + xy + \frac{1-m}{4} y^2 = 1$, welche den Namen *Pellsche Gleichung*[1]) trägt, stets eine ganzzahlige Lösung besitzt. Die bisherigen Entwicklungen lassen aber nicht erkennen, ob auch die Gleichungen $x^2 - my^2 = -1$ resp. $x^2 + xy + \frac{1-m}{4} y^2 = -1$ stets ganzzahlige rationale Lösungen besitzen. Nach später zu entwickeln-

---

1) Über die hist. Entwicklung bis zu Jacobi und Dirichlet vergl. man A. Konen, Geschichte der Gleichung $t^2 - Du^2 = 1$. Leipzig 1901. Die Aufgabe selbst, ganzzahlige rationale Lösungen der Gleichung $1 = x^2 - my^2$ zu bestimmen, ist sehr alt, in der neueren Zeit ist dieselbe zuerst von Fermat wieder gestellt und wahrscheinlich auch gelöst worden, nachdem die früheren Untersuchungen der Aufgabe vergessen waren (i. J. 1657, Fermat an Frenicle), s. Oeuvres de Fermat, t. II, p. 333.

Auf die scharfsinnige Behandlung der Aufgabe von Gauß, Disq. arithm. V, Art. 198—200 und 201, 202 möchte ich aber doch hier noch extra verweisen.

Über die numerische Behandlung der Pellschen Gleichung mit Hilfe von Kettenbrüchen (nach Lagrange) vergl. man Legendre, Zahlentheorie, Bd. I, p. 49 ff. (§ 5, 6) und ferner H. Schubert, Auslese aus meiner Unterrichts- und Vorlesungspraxis, Bd. II, Leipzig 1905, S. 160 ff.

den Sätzen lassen sich leicht unendlich viele Zahlen m bezeichnen, für welche die letzten Gleichungen sicher *nicht* durch ganze rationale Werte x, y *lösbar* sind. (Vergl. Nr. 24, I, S. 113.) Dagegen ist bis heute nur in speziellen Fällen die Frage entschieden, nach denjenigen Werten von m für welche auch jene Gleichungen notwendig durch rationale ganze Zahlen x, y befriedigt werden können. (Vergl. Nr. 23 und 32.)

Nachdem nun aber nachgewiesen ist, daß in einem reellen Körper jedenfalls Einheiten existieren, die von ± 1 verschieden sind, sieht man leicht, daß die sämtlichen Potenzen mit ganzzahligen positiven oder negativen Exponenten von einer solchen Einheit ε_r unendlich viele *von ε_r und unter sich verschiedene Einheiten* liefern.

Wenn nämlich ε irgend eine Einheit ist, so gilt auch für irgend welchen ganzzahligen Exponenten a die Gleichung:

$$n(\varepsilon^a) = (n(\varepsilon))^a = (\pm 1)^a,$$

also ist auch ε^a eine Einheit. Ist ferner a_1 irgend eine von a verschiedene ganze Zahl, dann sind auch ε^a und ε^{a_1} verschieden, denn für $|\varepsilon| \gtrless 1$ und $a > a_1 > 0$ ist:

$$|\varepsilon^a| \gtrless |\varepsilon^{a_1}|,$$

und für $a < a_1 < 0$ ist:

$$|\varepsilon^a| \lessgtr |\varepsilon^{a_1}|.$$

Es müssen also ε^a und ε^{a_1} voneinander verschieden ausfallen, ihr Quotient kann nicht ± 1 sein. Wenn man nun $\varepsilon^a = u + v\omega$ setzt, so ist $x = u$, $y = v$ eine Lösung der Gleichung (1) bezw. (2) für das $+$ oder $-$ Zeichen der rechten Seite.

Zu jeder Einheit ε, deren absoluter Betrag kleiner ist als 1, gibt es eine andere Einheit $\frac{1}{\varepsilon}$ für welche $\left|\frac{1}{\varepsilon}\right| > 1$ ausfällt.

Vorausgesetzt, daß die Gleichung

$$x^2 - my^2 = -1, \quad \text{resp.} \quad x^2 + xy + \frac{1-m}{4}y^2 = -1$$

eine Lösung besitzt, d. h. *wenn* es im Körper $k(\sqrt{m})$ eine Einheit ε_s gibt, für welche $n(\varepsilon_s) = -1$ ist, so liefern die ungeraden Potenzen derselben: ε_s^3, $\varepsilon_s^5 \ldots$ unendlich viele weitere Lösungen dieser selben Gleichung, weil $n(\varepsilon_s^{2a+1}) = -1$ ausfällt. Die geraden Potenzen dieser Einheit ε_s, nämlich ε_s^2, $\varepsilon_s^4 \ldots$, liefern dagegen unendlich viele verschiedene Lösungen der Gleichung

$$x^2 - my^2 = +1, \quad \text{resp.} \quad x^2 + xy + \frac{1-m}{4}y^2 = +1,$$

weil stets $n(\varepsilon_s^{2a}) = +1$ ist.

Die Einheiten, deren absolute Beträge > 1 sind, kann man nach der Größe dieser absoluten Beträge ordnen. Denn sind etwa η_1 und η_2 irgend zwei Einheiten der verlangten Art, für welche

$$|\eta_1| > 1, \quad |\eta_2| > 1$$

ist, so kann nur eine der beiden Ungleichungen

$$|\eta_1| \gtrless |\eta_2|$$

gelten, da die Gleichung $|\eta_1| = |\eta_2|$ nur erfüllt ist für $\eta_1 = \pm \eta_2$, wobei dann die beiden Einheiten nicht wesentlich verschieden wären.

Dieselbe Bemerkung, mit einer wesentlichen Ergänzung kann man auch direkt beweisen, durch Betrachtung der Gleichungen (1) resp. (2), welche zur Bestimmung der Einheiten dienen. Bedeuten nämlich x_1, y_1 und x_2, y_2 zwei positive rationale ganzzahlige Wertepaare, welche beide entweder der Gleichung $x^2 - my^2 = +1$ oder der Gleichung $x^2 - my^2 = -1$ genügen, so ist mit $y_1 \geqq y_2$ auch $x_1 \geqq x_2$ und mit $y_1 < y_2$ gleichzeitig $x_1 < x_2$. Wenn ferner die Gleichungen gelten $x_1^2 - my_1^2 = +1$ und $x_2^2 - my_2^2 = -1$, so ist analog für $y_1 \geqq y_2$ gleichzeitig $x_1 > x_2$ und für $y_1 < y_2$ auch $x_1 < x_2$.

Es bezeichne nun für den Fall $m \not\equiv 1, (4)$ der Ausdruck $\eta_i = \pm \bar{\eta} = x_i + y_i\sqrt{m}$ eine Einheit des Körpers $k(\sqrt{m})$, mit *positivem* x_i, $x_i > 0$, so ist sicher nur dann $|\eta_i| > 1$, falls auch y_i positiv ist. Wenn nun $\eta_1 = x_1 + y_1\sqrt{m}$ und $\eta_2 = x_2 + y_2\sqrt{m}$ zwei Einheiten dieser Art sind, so ist für $y_1 > y_2$ auch $|\eta_1| > |\eta_2|$ und umgekehrt.

Dasselbe Resultat erhält man für den zweiten Fall: $m \equiv 1, (4)$, wenn man die Einheit η_i in der Form $\eta_i = \left(x_i + \frac{y_i}{2}\right) + \frac{y_i}{2}\sqrt{m}$ schreibt und in der vorausgehenden Überlegung einfach $x_i + \frac{y_i}{2}$ statt x_i setzt.

Indem man daher die Lösungswerte der Gleichungen

$$x^2 - my^2 = \pm 1 \quad \text{resp.} \quad x^2 + xy + \frac{1-m}{4}y^2 = \pm 1$$

für das obere und falls es möglich ist für das untere Vorzeichen der rechten Seite bestimmt und die dadurch sich ergebenden Einheiten η_i mit der Bedingung $|\eta_i| > 1$ und positivem y_i nach der Größe der positiven Zahlen y_i ordnet, erhält man die absoluten Beträge der Einheiten selbst der Größe nach geordnet: $|\varepsilon| < \ldots < |\eta_1| < |\eta_2| \ldots$

Wenn in dieser Reihe der absoluten Beträge aller Einheiten $|\varepsilon|$ die kleinste Zahl bezeichnet, wo ε von jetzt ab eine, abgesehen vom

Faktor -1, ganz bestimmte Einheit des Körpers bedeutet, *dann stellt ε eine Grundeinheit des Körpers dar.*

In der Tat, versteht man unter η wieder eine beliebige Einheit des Körpers und ist zunächst $|\eta| > 1$, so läßt sich eine ganze positive Zahl e so finden, daß

$$|\varepsilon^e| \leqq |\eta| < |\varepsilon^{e+1}|,$$

also

$$1 \leqq \left|\frac{\eta}{\varepsilon^e}\right| < |\varepsilon|$$

ist. Da aber $\frac{\eta}{\varepsilon^e}$ auch eine Einheit des Körpers sein muß und da keine Einheit existiert, deren absoluter Betrag zwischen 1 und $|\varepsilon|$ gelegen ist, so kann allein die Gleichung gelten:

$$\left|\frac{\eta}{\varepsilon^e}\right| = 1,$$

d. h. es wird

$$\eta = \pm \varepsilon^e;$$

und auf genau dieselbe Weise zeigt man, daß eine Einheit, deren absoluter Betrag kleiner als 1 ist, gleich $\pm \frac{1}{\varepsilon^{e_1}}$ sein muß. Es ist also gezeigt, daß alle Einheiten des Körpers $k(\sqrt{m})$ sich in der Form

$$\pm \varepsilon^e$$

für alle ganzen rationalen Zahlen e darstellen lassen.[1])

Falls der Körper überhaupt Einheiten mit der Norm -1 enthält, so muß insbesondere auch die Grundeinheit ε eine negative Norm, $n(\varepsilon) = -1$ haben, denn wenn η eine Einheit mit positiver Norm bezeichnet, so gilt für alle Potenzen mit ganzzahligen Exponenten e stets die Gleichung $n(\pm \eta^e) = +1$. Schreibt man jetzt $\varepsilon = x + y\omega$ und setzt y positiv voraus, so sind y und x resp. y und $x + \frac{y}{2}$ die kleinsten positiven Lösungswerte der Gleichung $x^2 - my^2 = \pm 1$ resp. $x^2 + xy + \frac{1-m}{4} = \pm 1$ und zwar für das $+$ oder $-$ Zeichen der rechten Seite, wenn $n(\varepsilon) = +1$ oder $n(\varepsilon) = -1$ ist. Es genügen daher zur Bestimmung der Grundeinheit eine endliche Anzahl Rechenoperationen, da man die nötigen Lösungswerte der Gleichung (1) resp. (2) ev. durch Versuche oder durch die Methode der Kettenbruchentwicklung bestimmen kann. Ist von vornherein noch nicht sicher, ob die Norm

1) Disquis. arithmet. V, 200.

der Grundeinheit -1 ist, d. h. ob es eine ganzzahlige rationale Lösung der Gleichung:

$$x^2 - my^2 = -1, \quad \text{resp} \quad x^2 + xy + \frac{1-m}{4} y^2 = -1,$$

gibt, so kann man z. B. folgendermaßen verfahren: man berechne zunächst die Einheit η, mit der Norm $+1$ und der Bedingung $|\eta| > 1$ derart, daß $|\eta|$ den kleinsten Wert aller absoluten Beträge der Einheiten von derselben Art besitzt, durch die Bestimmung der absolut kleinsten Lösung der Gleichung:

$$x^2 - my^2 = +1, \quad \text{resp.} \quad x^2 + xy + \frac{1-m}{4} y^2 = +1,$$

und untersuche, ob die Gleichung $\eta = \pm \varepsilon^2 = \pm (x + y\omega)^2$ für ganzzahlige x, y auflösbar ist oder nicht. Je nachdem ist dann ε oder η selbst die Grundeinheit.

Zusammenfassend kann man jetzt die Sätze über die Einheiten so aussprechen:

In einem quadratischen Zahlkörper lassen sich alle Einheiten auf eine und nur eine Weise durch eine Grundeinheit ε in der Form:

$$\varrho\, \varepsilon^e$$

darstellen, wo ϱ eine dem Körper angehörige Einheitswurzel ev. ± 1 bedeutet und wo $\varepsilon = +1$ ist für die imaginären Körper und ε verschieden von 1 für die reellen Körper.

1. Beispiel. Für den Körper $k(\sqrt{3})$ ist $\varepsilon = 2 + \sqrt{3}$ eine Grundeinheit, denn die Gleichung

$$x^2 - 3y^2 = \pm 1$$

ist nur für das obere Zeichen lösbar, und es ergeben sich $x = 2$, $y = 1$ als die absolut kleinsten Lösungswerte dieser Gleichung; weitere Einheiten des Körpers sind:

$$\eta_1 = \varepsilon^2 = 7 + 4\sqrt{3}, \quad \eta_2 = \varepsilon^3 = 26 + 15\sqrt{3} \text{ usw.}$$

ferner:

$$\varepsilon' = \frac{1}{\varepsilon} = 2 - \sqrt{3},$$

$$\varepsilon'^2 = 7 - 4\sqrt{3}, \quad \varepsilon'^3 = 26 - 15\sqrt{3} \text{ usw.}$$

Für alle Einheiten des Körpers ist die Norm $+1$.

2. Beispiel, $k(\sqrt{14})$. Die absolut genommen kleinste ganzzahlige Lösung der Gleichung $x^2 - 14y^2 = +1$ ist $x = 15$, $y = 4$, und daher ist

$$\varepsilon = 15 + 4\sqrt{14}$$

die Grundeinheit des Körpers, weil die Gleichung $x^2 - 14y^2 = -1$ nicht lösbar ist. Weitere Einheiten sind z. B.:

$$\varepsilon^2 = 449 + 120\sqrt{14}, \quad \varepsilon^3 = 13455 + 3596\sqrt{14}$$

$$\varepsilon' = \frac{1}{\varepsilon} = 15 - 4\sqrt{14}$$

$$\varepsilon'^2 = 449 - 120\sqrt{14}, \quad \varepsilon'^3 = 13455 - 3596\sqrt{14}.$$

3. Beispiel, $k(\sqrt{5})$. Die kleinste ganzzahlige Lösung der Gleichung $x^2 + xy - y^2 = -1$ ist $x = 0$, $y = 1$, also wird

$$\begin{aligned} \varepsilon &= \omega \quad \text{und} & n(\varepsilon) &= -1 \\ \varepsilon^2 &= 1 + \omega, & n(\varepsilon^2) &= +1 \\ \varepsilon^3 &= 1 + 2\omega, & n(\varepsilon^3) &= -1, \end{aligned}$$

ferner ist

$$\varepsilon' = \frac{1}{\varepsilon} = \omega'.$$

An einer andern Stelle ergibt sich übrigens für den Fall $m \equiv 1, (4)$ die Tatsache, daß die Gleichungen $x^2 + xy + \frac{1-m}{4}y^2 = \pm 1$ und $x_1^2 - my_1^2 = \pm 1$ für das + ev. — Zeichen immer gleichzeitig lösbar sind (vergl. Nr. 33).

23. Körper mit ungerader Klassenanzahl.

Satz.[1]) *Jede ganze oder gebrochene Zahl α des Körpers $k(\sqrt{m})$, deren Norm gleich $+1$ ist, läßt sich als Quotient zweier ganzer zueinander konjugierten Zahlen des Körpers in der Form $\frac{\gamma}{\gamma'}$ darstellen.*

Beweis. Für eine ganze oder gebrochene Zahl α des Körpers $k(\sqrt{m})$ kann man jedenfalls setzen:

$$\alpha = \frac{a}{c} + \frac{b}{c}\omega,$$

wo nun a, b, c ganze rationale Zahlen sind. Wegen $n(\alpha) = +1$ sind a und b prim zueinander, wenn man von vornherein ausschließt, daß a, b, c einen gemeinsamen Teiler besitzen.

Zum Beweise des Satzes unterscheiden wir die beiden Fälle $m \equiv 1$ und $m \not\equiv 1, (4)$.

1. Fall. $m \not\equiv 1, (4)$; dann ist $\omega = \sqrt{m}$. Setzt man die Gleichung an:

$$\alpha = \frac{1}{c}(a + b\omega) = \frac{x + y\omega}{x + y\omega'}, \tag{1}$$

1) Hilbert, Zahlb. Cap. XV, § 54.

so ergeben sich für die Berechnung von x und y zwei lineare Gleichungen:

$$\left(\frac{a}{c}-1\right)x-\frac{b}{c}\,my=0 \tag{2}$$

$$\frac{b}{c}\,x-\left(\frac{a}{c}+1\right)y=0. \tag{3}$$

Diese Gleichungen sind aber durch zwei ganze rationale von 0 verschiedene Zahlen lösbar, wenn ihre Determinante $\varDelta$ verschwindet. Nun ist

$$\varDelta=-\frac{a^2}{c^2}+1+\frac{b^2}{c^2}\,m=1-n(\alpha)=0, \tag{4}$$

also kann man wählen

$$x=\frac{1}{t}(a+c),\quad y=\frac{1}{t}\,b, \tag{5}$$

wenn t einen gemeinsamen Teiler der Zahlen $a+c$ und b bedeutet.

2. Fall. $m\equiv 1,\ (4),\ \omega=\frac{1+\sqrt{m}}{2},\ \omega'=\frac{1-\sqrt{m}}{2}.$ Es sei wieder $\alpha=\frac{1}{c}(a+b\omega)$ und man setze:

$$\frac{a}{c}+\frac{b}{c}\,\omega=\frac{x+y\omega}{x+y\omega'}, \tag{1}$$

dann genügen x und y den beiden linearen Gleichungen:

$$\left(\frac{a}{c}-1\right)x+\left(\frac{a}{c}+\frac{b}{c}\,\frac{1-m}{4}\right)y=0 \tag{2}$$

$$\frac{b}{c}x-\left(\frac{a}{c}+1\right)y=0, \tag{3}$$

und diese besitzen wieder ein gemeinsames Lösungssystem von zwei ganzen rationalen von Null verschiedenen Zahlen x, y, wenn ihre Determinante $\varDelta$ verschwindet. Nun ist aber in der Tat auch:

$$\varDelta=-\frac{a^2}{c^2}+1-\frac{ab}{c^2}-\frac{b^2}{c^2}\,\frac{1-m}{4}=1-n(\alpha)=0 \tag{4}$$

nach der Voraussetzung über α.

Wie im früheren Fall kann man daher auch jetzt für x, y wieder setzen:

$$x=\frac{1}{t}(a+c),\quad y=\frac{1}{t}\,b. \tag{5}$$

Es hat also in beiden Fällen die gesuchte ganze Zahl γ die folgende Form:

$$\gamma=\frac{1}{t}\left\{a+c+b\omega\right\}=\frac{c}{t}\left\{1+\alpha\right\}.$$

Anmerkung. Der Leser möge den Beweis des Satzes auch direkt führen, ausgehend von der letzten Gleichung.

Wenn insbesondere α eine *ganze* Zahl des Körpers und folglich eine Einheit ist, so kann man für γ den Ausdruck $1 + \varepsilon$ wählen.

Eine bemerkenswerte Folgerung dieses Satzes ist die Tatsache, die der folgende Satz[1]) ausspricht:

Satz. *Wenn die Diskriminante eines reellen Körpers $k(\sqrt{m})$ nur eine einzige Primzahl enthält, so ist die Norm der Grundeinheit dieses Körpers gleich* -1.

Beweis. Die Voraussetzung des Satzes trifft nur zu, wenn entweder $m = 2$ ist, oder wenn m eine ungerade Primzahl von der Form $p \equiv 1$, (4) ist.

Die Grundeinheit des Körpers sei ε. Angenommen nun, es wäre $n(\varepsilon) = +1$, dann existiert nach dem eben bewiesenen Satz eine ganze Zahl γ des Körpers von der Art, daß man $\varepsilon = \frac{\gamma}{\gamma'}$ setzen kann. γ ist eine ganze Zahl, für welche die Idealgleichung

$$(\gamma) = (\gamma') \quad \text{oder} \quad (\gamma) = (\gamma)'$$

besteht. Jedes Ideal des Körpers, das in (γ) aufgeht, muß folglich auch in dem konjugierten Ideal (γ') aufgehen. Da aber die Diskriminante des Körpers nur eine einzige Primzahl enthält, so ist (auch für $m = 2$) das einzige ambige Ideal des Körpers, welches seinem konjugierten Ideal gleich ist, das Ideal $(\sqrt{m})$, und die Zahl γ kann daher außer ganzen rationalen Faktoren und Einheiten nur die Zahl $\sqrt{m}$ enthalten. D. h. man kann

$$(\gamma) = (a) \qquad \text{oder} \quad \gamma = \eta a, \text{ resp.}$$
$$(\gamma) = (\sqrt{m}) \quad \text{oder} \quad \gamma = \eta\sqrt{m}$$

setzen, wobei η eine von 1 verschiedene Einheit des Körpers bezeichnet. Dann wird aber in beiden Fällen:

$$\varepsilon = \frac{\eta\sqrt{m}}{-\eta'\sqrt{m}} = \pm\,\eta^2,$$

und folglich wäre ε nicht die Grundeinheit des Körpers, wie der Satz voraussetzt.

Auf Grund des vorhergehenden Satzes, welcher eine sehr bemerkenswerte Ergänzung zu dem Satz über die Existenz der Einheiten in Nr. 16 bildet, ist es möglich, einen weiteren Satz zu beweisen,

1) Hilbert, Zahlb. Cap. XVII, § 68. Dieser Satz ist auf ganz andere Weise von P. Lejeune-Dirichlet bewiesen worden; vergl. Werke Bd. I, S. 224.

welcher sich später als Spezialfall eines viel allgemeineren Fundamentalsatzes erweisen wird. Es gilt nämlich die folgende Behauptung:

Satz. *Wenn die Diskriminante eines Zahlkörpers $k(\sqrt{m})$ nur eine Primzahl p enthält, so ist die Klassenanzahl h des Körpers ungerade.*

Beweis. Es werde, entgegen der Behauptung, die Klassenanzahl h gerade vorausgesetzt, dann gibt es sicher ein Nichthauptideal $\mathfrak{j}$, dessen Quadrat ein Hauptideal ist. Aus den beiden alsdann geltenden Äquivalenzen

$$\mathfrak{j}^2 \sim 1, \quad \mathfrak{j}\mathfrak{j}' \sim 1$$

folgt aber $\mathfrak{j} \sim \mathfrak{j}'$. Darnach darf man $\frac{\mathfrak{j}}{\mathfrak{j}'} = \alpha$ setzen, wo α eine ganze oder gebrochene Zahl des Körpers bezeichnet, deren Norm $n(\alpha) = \pm 1$ ist.

Für einen imaginären Körper ist sicher $n(\alpha) = 1$, für einen reellen Körper ist entweder $n(\alpha) = +1$ oder $n(\varepsilon\alpha) = +1$, wenn ε die Grundeinheit bezeichnet, weil ja $n(\varepsilon) = -1$ ist. Falls $n(\alpha) = +1$ ist, darf jetzt wieder $\alpha = \frac{\gamma}{\gamma'}$ gesetzt werden, falls $n(\alpha) = -1$ ist, so setze man $\varepsilon\alpha = \frac{\gamma}{\gamma'}$. In allen Fällen folgt somit aus der Annahme $\mathfrak{j}^2 \sim 1$ eine Gleichung $(\gamma)\mathfrak{j} = (\gamma\mathfrak{j})'$. Jedes Ideal, das in dem Ideal $(\gamma)\mathfrak{j}$ aufgeht, muß folglich auch in dem konjugierten Ideal $(\gamma\mathfrak{j})'$ aufgehen, d. h. es ist $(\gamma\mathfrak{j})$ nur durch ambige Ideale und rationale Hauptideale teilbar. Da nun der Körper $k(\sqrt{-1})$ das ambige Ideal $(1+\sqrt{-1})$, jeder andere Körper $k(\sqrt{m})$ (für $m = 2$ oder $m \equiv 1, (4)$) nur das ambige Ideal $(\sqrt{m})$ enthält, so ergibt sich $(\gamma)\mathfrak{j}$ entweder gleich (a), oder gleich $(a\sqrt{m})$ bezw. gleich $\left(a \cdot (1+\sqrt{-1})\right)$ für $m = -1$. Für alle diese Möglichkeiten folgt aber hieraus $\mathfrak{j} \sim 1$, und damit ist die Annahme des Beweisganges widerlegt, es gilt vielmehr: die Klassenanzahl h ist ungerade.

Ich schalte an dieser Stelle einige spezielle Betrachtungen ein. Es wäre jetzt wohl möglich die Untersuchung der Körper $k(\sqrt{-1})$, $k(\sqrt{\pm 2})$ u. a. durchzuführen. Unser nächster Zweck ist aber der Beweis des mehrfach erwähnten quadratischen Reziprozitätsgesetzes, und es soll daher die Betrachtung einiger einfacher Körper nur so weit durchgeführt werden, als es für jenen Zweck erforderlich ist.

24. Ergänzungssätze zum quadratischen Reziprozitätsgesetz.

I. Der einfachste, von Gauß in seiner Theorie der biquadratischen Reste zuerst betrachtete Zahlkörper ist der Körper $k(\sqrt{-1})$.

Für diesen Körper gilt noch das Gesetz von der eindeutigen Zerlegung der Zahlen in Primfaktoren, man hat $h = 1$ und es sind darum auch die Eigenschaften dieses Körpers sehr einfach. Hier soll nur untersucht werden, welche rationalen Primzahlen im Körper zerfallen, und welche Primzahlen auch in dem neuen Bereich $k(\sqrt{-1})$ unzerlegbar bleiben.

1. Wenn eine ungerade rationale Primzahl p im Körper $k(\sqrt{-1})$ in ein Produkt aus zwei Primidealen ersten Grades $(p) = \mathfrak{p} \cdot \mathfrak{p}'$ zerfällt, so gibt es eine und nur eine einzige Darstellung:

$$p = (x + \sqrt{-1}\, y)(x - \sqrt{-1}\, y),$$

oder es ist:

$$p = x^2 + y^2.$$

Die Zahl p ist nach Voraussetzung ungerade, also können x und y nicht beide ungerade sein, ferner können x, y nicht zugleich gerade sein oder irgend einen anderen gemeinsamen Faktor besitzen. Die Darstellung $p = x^2 + y^2$ ist nur möglich, wenn etwa x ungerade und y gerade ist, und damit ergibt sich als eine *notwendige* Bedingung für die Zerfällbarkeit von p: es muß $p \equiv 1,\ (4)$ sein.

2. Diese Bedingung ist aber auch *hinreichend*, d. h. wenn p eine ungerade Primzahl darstellt und $p \equiv 1,\ (4)$ ist, so zerfällt p im Körper $k(\sqrt{-1})$. Es besitzt alsdann nämlich der quadratische Körper $k(\sqrt{p})$ eine Grundeinheit ε, deren Norm -1 ist, und dies heißt, daß die Gleichung

$$\left(x + \frac{y}{2}\right)^2 - \frac{p}{4}\, y^2 = -1, \tag{1}$$

folglich auch die Kongruenz

$$(2x + y)^2 + 4 \equiv 0,\ (p) \tag{2}$$

durch ganze rationale Zahlen x und y befriedigt werden kann. Wählt man eine ganze rationale Zahl z entsprechend der Kongruenz

$$2z \equiv 1,\ (p) \tag{3}$$

und multipliziert die Kongruenz (2) mit z^2, so folgt, daß mit der Kongruenz $(2x + y)^2 + 4 \equiv 0,\ (p)$ zugleich auch die Kongruenz $X^2 + 1 \equiv 0,\ (p)$ lösbar ist und umgekehrt. Sei nun $X = a$ eine Lösung der Kongruenz $X^2 + 1 \equiv 0,\ (p)$, dann zerfällt, wie in Nr. 14,

S. 59 ff., gezeigt wurde, das Ideal (p) in zwei verschiedene Primideale $(p) = (p,\ a + \sqrt{-1})\,(p,\ a - \sqrt{-1})$. Diese Primideale müssen indes Hauptideale sein und man erhält also $p = (x + \sqrt{-1}\,y)\,(x - \sqrt{-1}\,y)$.

Da eine Primzahl $p \equiv 3,\ (4)$ im Körper $k(\sqrt{-1})$ *nicht* zerfällt, so folgt ferner, daß die Kongruenz $x^2 + 1 \equiv 0,\ (p)$ nicht lösbar sein kann, wenn $p \equiv 3,\ (4)$.

3. Die Zahl 2, welche in der Diskriminante $d = -4$ des Körpers aufgeht, zerfällt nach folgender Gleichung:

$$2 = (1 + \sqrt{-1})\,(1 - \sqrt{-1}),$$

oder es ist

$$(2) = (1 + \sqrt{-1})^2 = (1 - \sqrt{-1})^2,$$

indem $(1 \pm \sqrt{-1})$ ambige Ideale des Körpers sind.

Die Resultate dieser Betrachtungen kann man auch in den folgenden Sätzen aussprechen:

Satz. *Jede rationale positive Primzahl p von der Form $4n + 1$ läßt sich auf eine einzige Weise als Summe zweier Quadratzahlen*[1])

$$p = x^2 + y^2$$

darstellen.

Eigentlich wieder ein spezieller Fall hiervon ist der folgende Satz:

Satz. *Die quadratische Kongruenz*

$$x^2 + 1 \equiv 0,\ (p)$$

ist dann und nur dann lösbar, wenn p von der Form $4n + 1$ ist, oder eine Zahl von der Gestalt $x^2 + 1$ kann nur Divisoren von der Form $4n + 1$ besitzen. (Eine Erweiterung dieses Satzes siehe S. 122.)

Endlich: *Es ist* $\left(\frac{-1}{p}\right) = +1$ *für eine ungerade Primzahl* $p \equiv 1,\ (4)$ *und* $\left(\frac{-1}{p}\right) = -1$ *für* $p \equiv 3,\ (4)$, *was man in der Formel*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

zusammenfassen kann.

Es ist übrigens leicht, dieses Resultat elementar zu beweisen, z. B. aus der Eulerschen Kongruenz $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}},\ (p)$, wir haben aber den vorstehenden Beweis gewählt, da dieser der weitgehendsten Verallgemeinerung fähig ist.

---

1) Dieser Satz stammt schon von Fermat und ist von Euler zuerst bewiesen worden.

Schließlich kann man aus dem letzten Satz noch eine sehr wichtige Folgerung ziehen: Wenn m eine ganze rationale Zahl ist, welche Primfaktoren von der Form $p \equiv 3$, (4) enthält, so kann die Kongruenz $x^2 + 1 \equiv 0$, (m) und umsomehr die Diophantische Gleichung $x^2 - my^2 = -1$ resp. $x^2 + xy + \frac{1-m}{4} y^2 = -1$ *nicht lösbar* sein, d. h. *die Grundeinheit* ε *eines Körpers* $k(\sqrt{m})$, *dessen Grundzahl Primfaktoren der Form* $p \equiv 3$, (4) *enthält, hat stets die Norm* $n(\varepsilon) = +1$.

II. Der Körper $k(\sqrt{2})$. Alle Ideale des Körpers sind Hauptideale, und es soll wieder die Frage behandelt werden nach denjenigen rationalen Primzahlen p, welche in dem Körper $k(\sqrt{2})$ in ein Produkt aus zwei Primzahlen ersten Grades zerfallen.

1. Wenn p eine ungerade Primzahl ist, welche in $k(\sqrt{2})$ zerfällt, so gibt es ganze rationale Zahlen x, y, welche die Gleichung erfüllen:

$$+p = x^2 - 2y^2.$$

Denn für die Grundeinheit $\varepsilon = 1 + \sqrt{2}$ ist $n(\varepsilon) = -1$, und es sind daher die Gleichungen $p = x^2 - 2y^2$ und $-p = x_1^2 - 2y_1^2$ stets gleichzeitig lösbar oder unlösbar.

Ist nämlich $(p) = (x + y\sqrt{2})(x - y\sqrt{2})$, und zwar so, daß $+p = x^2 - 2y^2$ gesetzt werden muß, dann ist auch:

$$(p) = (x + y\sqrt{2})(1 + \sqrt{2})(x - y\sqrt{2})(1 - \sqrt{2}),$$

oder

$$-p = (x + 2y)^2 - 2(x + y)^2 = x_1^2 - 2y_1^2.$$

Die Diophantische Gleichung $p = x^2 - 2y^2$ kann aber für ein ungerades p nur in der Weise lösbar sein, daß x ungerade und y entweder gerade oder ungerade ist; das ergibt als *notwendige* Bedingung für die Zerlegbarkeit der Primzahl p im Körper $k(\sqrt{2})$:

$$p \equiv 1, (8) \quad \text{oder} \quad p \equiv 7, (8).$$

2. Diese Bedingung ist auch *hinreichend:*

Falls p eine ungerade Primzahl ist, für welche $p \equiv 1$ oder $p \equiv 7$, (8) ist, so zerfällt dieselbe im Körper $k(\sqrt{2})$.

Schreibt man $p_1 = p$, wenn $p \equiv 1$, (8) ist, ferner $p_1 = -p$, wenn $p \equiv 7$, (8), dann ist für beide Fälle $p_1 \equiv 1$, (8), und es besitzt der Körper $k(\sqrt{p_1})$ eine ungerade Klassenanzahl h, weil die Diskriminante dieses Körpers nur die einzige Primzahl $\pm p_1$ als Faktor besitzt. Bezeichnen $1, \omega = \frac{1 + \sqrt{p_1}}{2}$ die Basiszahlen des Körpers $k(\sqrt{p_1})$, dann gelten für das Ideal (2) die Zerlegungen:

$$(2) = (2,\ 1 + \omega)(2,\ 1 + \omega') = \mathfrak{p} \cdot \mathfrak{p}',$$

bezw.

$$(2) = (2,\ \omega)(2,\ \omega') = \mathfrak{p} \cdot \mathfrak{p}',$$

in die zwei voneinander verschiedenen Primideale $\mathfrak{p}$ und $\mathfrak{p}'$. Weil nun nach Voraussetzung die Klassenanzahl h ungerade ist, so existiert sicher eine *ungerade* Zahl $2g + 1$, Faktor von h, für welche $\mathfrak{p}^{2g+1}$ und $\mathfrak{p}'^{2g+1}$ Hauptideale werden. Man kann daher jedenfalls x, y als ganze rationale Zahlen annehmen derart, daß

$$\mathfrak{p}^{2g+1} = (x + y\omega), \quad \mathfrak{p}'^{2g+1} = (x + y\omega')$$

und

$$+\ 2^{2g+1} = x^2 + xy + y^2\frac{1-p_1}{4}$$

ausfällt. Aus dieser Gleichung gewinnt man durch ein ganz gleiches Schlußverfahren wie unter (I, 2) die Tatsache, daß die Kongruenz

$$(2x + y)^2 - 4 \cdot 2^{2g+1} \equiv 0,\ (p_1)$$

und folglich auch die Kongruenz

$$z^2 - 2 \equiv 0,\ (p_1)$$

lösbar ist.

Bezeichnet $z = a$ eine Wurzel dieser Kongruenz, so ergibt sich

$$(p_1) = (p_1,\ a - \sqrt{2})(p_1,\ a + \sqrt{2});$$

weil der Körper $k(\sqrt{2})$ die Klassenanzahl 1 hat, sind die beiden voneinander und von (p_1) verschiedenen Faktoren auf der rechten Seite der letzten Gleichung konjugierte Hauptideale, also ist

$$(p_1) = (x + y\sqrt{2})(x - y\sqrt{2}).$$

Ferner folgt, daß die Kongruenz $x^2 - 2 \equiv 0,\ (p)$ auch nur für die Fälle $p \equiv \pm 1,\ (8)$ lösbar sein kann.

3. Für die Zahl 2 gilt einfach

$$(2) = (\sqrt{2})^2,$$

wie es der allgemeine Satz verlangt.

Indem ich auf die in den letzten Gleichungen steckenden Sätze in einem andern Zusammenhang nochmals zurückkommen will, soll zunächst nur der folgende Satz herausgefaßt werden:

Satz. *Die quadratische Kongruenz*

$$x^2 - 2 \equiv 0,\ (p)$$

ist stets und nur dann durch ganze Zahlen lösbar, wenn $p \equiv \pm 1,\ (8)$ *ist.*

Oder: Eine ganze Zahl von der Form $x^2 - 2$ besitzt nur Divisoren von der Form $8n \pm 1$.

Oder schließlich: Es ist $\left(\frac{2}{p}\right) = +1$, wenn p eine ungerade

Primzahl von der Form $8n \pm 1$ ist, und es wird $\left(\frac{2}{p}\right) = -1$, wenn $p \equiv \pm 3, (8)$ ist. Diese beiden Formeln kann man zusammenfassen in eine einzige:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

III. Durch eine ähnliche Betrachtung des noch einfacheren Körpers $k(\sqrt{-2})$ gelangt man zu der folgenden Tatsache:

Satz. *Die quadratische Kongruenz*

$$x^2 + 2 \equiv 0, \ (p)$$

ist lösbar für die ungeraden Primzahlen $p \equiv 1$ *und* $p \equiv 3, (8)$, *und unlösbar für* $p \equiv 5$, $p \equiv 7, (8)$.

Oder es ist $\left(\frac{-2}{p}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}}$.

Die so aus der Körpertheorie abgeleiteten Gleichungen

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{und} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

heißen die *Ergänzungssätze* zum quadratischen Reziprozitätsgesetz.

Der zuletzt entwickelte Satz über den Restcharakter der Zahl -2 nach p läßt sich übrigens viel einfacher ableiten, indem man von der Gleichung $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ ausgeht, denn es ist $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$.

25. Das quadratische Reziprozitätsgesetz für die ungeraden rationalen Primzahlen.

Unsere Entwicklungen sind nun so weit vorgeschritten, daß dieses Gesetz, das „*theorema fundamentale*“ von Gauß, abgeleitet werden kann.

Sind p, q irgendwelche *ungerade* verschiedene Primzahlen, so liegt es jetzt, nachdem die Bestimmung von $\left(\frac{-1}{p}\right)$ und $\left(\frac{\pm 2}{p}\right)$ gelungen ist, doch nahe, allgemein nach dem Werte von $\left(\frac{p}{q}\right)$ zu fragen. Die Beantwortung dieser Frage hängt aber aufs engste zusammen mit der Tatsache, welche zuerst Euler[1]) (Opusc. anal. 1, 1783, p. 64) entdeckt hat, daß zwischen den Lösungsmöglichkeiten der beiden Kongruenzen

1) Die hier angeführten Daten aus der Geschichte der Entdeckung des quadratischen Reziprozitätsgesetzes sind einer geschichtlichen Darstellung von P. Bachmann, Niedere Zahlentheorie, Teil I, Leipzig 1902, S. 200ff. entnommen. Man vergl. außerdem O. Baumgart, Zeitschr. f. Math. u. Physik, hist. Abteilung, 1885, Band 30, S. 169: Über das quadratische Reziprozitätsgesetz. Eine vergleichende Darstellung der Beweise usw.

$$x^2 - q \equiv 0,\ (p) \quad \text{und} \quad x^2 - p \equiv 0,\ (q)$$

eine leicht angebbare Wechselbeziehung, Reziprozität, besteht, welche Legendre 1785 [und 1798] wieder entdeckt und auf die Form gebracht hat

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Diese Formel enthält in einfachster Weise das *quadratische Reziprozitätsgesetz*, mit dessen Beweis sich seit Gauß zahlreiche Mathematiker beschäftigt haben.

Der folgende Beweis des Reziprozitätsgesetzes folgt im Prinzip einem Beweis von Kummer (2. Beweis in den Abhandl. der kgl. Akad. Berlin, 1861), vergl. Hilbert, Zahlber. Cap. XVII, § 68—69.

Zur bequemeren Darstellung des Beweises setze ich eine besondere Bezeichnung fest: Es mögen p, q positive ungerade Primzahlen bezeichnen, insbesondere sollen p, p_1, p_2 ... stets Primzahlen $\equiv 1$, (4) und q, q_1, q_2 ... Primzahlen $\equiv 3$, (4) sein. Dann sind im Beweise die verschiedenen Kombinationen der Primzahlen p, q zu unterscheiden. Man hat offenbar die drei Fälle der Kombinationen: p, p_1, ferner p, q und schließlich q, q_1 auseinanderzuhalten.

1. Fall. Wenn die quadratische Kongruenz

$$x^2 - p \equiv 0,\ (p_1)$$

lösbar ist, wenn also $\left(\frac{p}{p_1}\right) = +1$ ausfällt, so ist p_1 im Körper $k(\sqrt{p})$ in zwei verschiedene Primideale ersten Grades zerlegbar, und es kann gesetzt werden:

$$(p_1) = (p_1,\ a + \omega)(p_1,\ a + \omega') = \mathfrak{p} \cdot \mathfrak{p}'.$$

Da aber die Klassenanzahl h des Körpers $k(\sqrt{p})$ ungerade ist, indem die Diskriminante des Körpers nur die einzige Primzahl p enthält, so gibt es stets eine ungerade Zahl $h_1 = 2g + 1$, welche ein Teiler ist von h, derart, daß die h_1^{te} Potenz von $\mathfrak{p}$ sowohl wie von $\mathfrak{p}_1$ Hauptideale werden. Weil außerdem die Norm der Grundeinheit ε des Körpers $k(\sqrt{p})$ gleich -1 ist, so darf man setzen:

$$p_1^{2g+1} = (x + y\omega)(x + y\omega'),$$

oder:

$$p_1^{2g+1} = \left(x + \frac{y}{2}\right)^2 - \frac{p}{4}y^2,$$

woraus die Kongruenz folgt:

$$(2x + y)^2 - p_1(2p_1^g)^2 \equiv 0,\ (p).$$

Hieraus schließt man wie oben, daß auch die Kongruenz

$$z^2 - p_1 \equiv 0,\ (p),$$

oder anders geschrieben:

$$x^2 - p_1 \equiv 0, \ (p)$$

lösbar ist.

Wenn also $\left(\frac{p}{p_1}\right) = +1$ ist, so ist hiernach auch $\left(\frac{p_1}{p}\right) = +1$.

Daraus folgt nun weiter, daß, wenn $\left(\frac{p}{p_1}\right) = -1$ ist, auch gleichzeitig $\left(\frac{p_1}{p}\right) = -1$ sein muß. In der Tat würde ja aus der Gleichung $\left(\frac{p_1}{p}\right) = +1$ rückwärts folgen, daß $\left(\frac{p}{p_1}\right) = +1$ ist, im Widerspruch mit der gegebenen Gleichung.

2. **Fall.** Es liege nun eine Kongruenz $x^2 - p \equiv 0, \ (q)$ vor.

Setzt man $\left(\frac{p}{q}\right) = +1$ voraus, so daß also q im Körper $k(\sqrt{p})$ zerlegbar ist, entsprechend der Gleichung:

$$(q) = (q, \ a + b\omega)(q, \ a + b\omega'),$$

dann kann wieder aus der Tatsache, daß die Klassenanzahl des Körpers $k(\sqrt{p})$ ungerade ist und für diesen Körper $n(\varepsilon) = -1$ wird, gefolgert werden, daß für ganze rationale Zahlen x, y eine Gleichung besteht:

$$q^{2g+1} = \left(x + \frac{y}{2}\right)^2 - \frac{p}{4} y^2,$$

oder daß die Kongruenz:

$$x^2 - q \equiv 0, \ (p),$$

in ganzen Zahlen lösbar ist.

Die Gleichung $\left(\frac{p}{q}\right) = +1$, hat also die Gleichung $\left(\frac{q}{p}\right) = +1$ zur Folge.

Nun ist aber umgekehrt zu zeigen, daß mit $\left(\frac{q}{p}\right) = +1$ auch notwendig $\left(\frac{p}{q}\right) = 1$ sein muß.

Wenn $\left(\frac{q}{p}\right) = +1$, also die Kongruenz

$$x^2 - q \equiv 0, \ (p)$$

lösbar ist, so ist nämlich (wie übrigens schon aus der Gleichung $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)$ folgt) auch die Kongruenz

$$x^2 + q \equiv 0, \ (p)$$

lösbar. Denn es gibt eine ganze rationale zu p prime Zahl z, so daß $z^2 \equiv -1, \ (p)$ wird, es besteht also mit der Kongruenz

$$x^2 - q \equiv 0, \ (p),$$

zugleich auch die andere:

$$(zx)^2 - z^2 q \equiv 0, \ (p)$$

in ganzen Zahlen z, xz. Oder wenn

$$X \equiv zx \quad \text{und} \quad z^2 \equiv -1, \ (p)$$

gesetzt werden, so ist also:

$$X^2 + q \equiv 0, \ (p).$$

Da jetzt $\left(\frac{-q}{p}\right) = +1$ ausfällt, so ist p in dem imaginären Körper $k(\sqrt{-q})$ zerlegbar, und da nun $-q \equiv 1$, (4) ist, so ist die Klassenanzahl des Körpers $k(\sqrt{-q})$ wiederum ungerade und man schließt wie in den vorhergehenden Fällen und unter Berücksichtigung der Tatsache, daß die Norm einer ganzen Zahl des imaginären Körpers $k(\sqrt{-q})$ stets positiv sein muß, daß alsdann die Kongruenz

$$x^2 - p \equiv 0, \ (q)$$

ebenfalls lösbar ist.

Zusammenfassend kann man daher sagen:

a) wenn $\left(\frac{p}{q}\right) = +1$ ist, so ist auch $\left(\frac{q}{p}\right) = +1$ und

b) wenn $\left(\frac{q}{p}\right) = +1$ ist, so muß auch $\left(\frac{p}{q}\right) = +1$ sein.

Daraus ergibt sich schließlich: wenn $\left(\frac{p}{q}\right) = -1$ ist, so muß auch $\left(\frac{q}{p}\right) = -1$ sein und umgekehrt.

Würde im Gegenteil angenommen, daß mit $\left(\frac{p}{q}\right) = -1$ gleichzeitig $\left(\frac{q}{p}\right) = +1$ ist, so würde aus letzterer Gleichung rückwärts folgen, daß auch $\left(\frac{p}{q}\right) = +1$ sein muß, was offenbar ein Widerspruch zu der ersten Annahme ist.

3. Fall. Die beiden gegebenen Primzahlen seien q und q_1.

Wird zunächst $\left(\frac{q}{q_1}\right) = -1$ gesetzt, so folgt nach dem Produktsatz für das Legendresche Symbol wegen $\left(\frac{-1}{q_1}\right) = -1$, daß dann

$$\left(\frac{-q}{q_1}\right) = +1$$

ist. Die Primzahl q_1 ist daher in dem imaginären Körper $k(\sqrt{-q})$ zerfällbar, und da dieser Körper wegen $-q \equiv 1$, (4) eine Diskriminante mit nur einem Primfaktor besitzt, so ist seine Klassenanzahl ungerade, es ergibt sich analog wie im vorhergehenden Fall:

$$\left(\frac{q_1}{q}\right) = +1.$$

Wenn nun aber $\left(\frac{q}{q_1}\right) = +1$ vorausgesetzt wird, versagt die bisherige Schlußweise zur Bestimmung von $\left(\frac{q_1}{q}\right)$. Nach Herrn Hilbert betrachtet man dann den Körper $k(\sqrt{q q_1})$. Für diesen Körper ist $m = q \cdot q_1 \equiv 1$, (4) und $d = q q_1$. Die einzigen Primzahlen, welche durch Quadrate von Primidealen teilbar sind, sind q und q_1. Setzt man $(q) = \mathfrak{q}^2$, $(q_1) = \mathfrak{q}_1^2$, so sind $\mathfrak{q}$, $\mathfrak{q}_1$, $\mathfrak{q}\mathfrak{q}_1$ die einzigen ambigen Ideale des Körpers, $\mathfrak{q}\mathfrak{q}_1$ ist ein Hauptideal, und es läßt sich durch eine Zwischenbetrachtung zeigen, daß auch $\mathfrak{q}$ und $\mathfrak{q}_1$ Hauptideale sind, woraus dann der Wert von $\left(\frac{q_1}{q}\right)$ folgt.

ε bezeichne die Grundeinheit des Körpers $k(\sqrt{q q_1})$, dann muß $n(\varepsilon) = +1$ sein, weil $\left(\frac{-1}{q}\right) = -1$, $\left(\frac{-1}{q_1}\right) = -1$ ist. Man kann nun nach dem Satz auf S. 107 eine ganze nicht rationale Zahl α des Körpers angeben, so daß $\varepsilon = \frac{\alpha}{\alpha'}$ oder $(\alpha) = (\alpha')$ wird. Das Ideal (α) ist somit ein Ideal von der Art, daß jedes Ideal, das in (α) aufgeht, auch in $(\alpha)'$ aufgehen muß. Bedeutet jetzt η eine Einheit des Körpers, für welche $\alpha = \eta \cdot a$ oder $\alpha = \eta \cdot \sqrt{q q_1}$ gesetzt werden kann, dann wäre:

$$\varepsilon = \frac{\alpha}{\alpha'} = \frac{\eta a}{\eta' a} = \pm \eta^2, \quad \text{oder} \quad \varepsilon = \frac{\eta \sqrt{q q_1}}{-\eta' \sqrt{q q_1}} = \pm \eta^2,$$

und dies widerspricht der Annahme, daß ε eine Grundeinheit ist. Nachdem aber ausgeschlossen ist, daß α durch $\mathfrak{q}$ und $\mathfrak{q}'$ zugleich teilbar ist, bleiben nur noch die Möglichkeiten übrig:

$$(\alpha) = (a)\mathfrak{q} \quad \text{oder} \quad (\alpha) = (a)\mathfrak{q}_1,$$

und in beiden Fällen ist daher

$$\mathfrak{q} \sim 1, \quad \mathfrak{q}_1 \sim 1.$$

Geht man von den Idealen $\mathfrak{q}_1$ oder $\mathfrak{q}$ zur Norm über, so folgt

$$\pm q_1 = \left(x + \frac{y}{2}\right)^2 - \frac{q q_1}{4} y^2,$$

oder

$$\pm 4 q_1 = (2x + y)^2 - q q_1 y^2.$$

Diese Gleichung ist nur möglich, wenn $2x + y$ durch q_1 teilbar ist, und dann kann man dieselbe einfacher auch so schreiben:

$$\pm 4 = q_1 X^2 - q Y^2.$$

Um über das Vorzeichen der linken Seite zu entscheiden, benützt man jetzt die Voraussetzung, daß $\left(\frac{q}{q_1}\right) = +1$ ist. Schreibt man nämlich die vorige Gleichung als Kongruenz:

$$q Y^2 \pm 4 \equiv 0, \ (q_1),$$

oder

$$Y_1^2 \pm 4q \equiv 0, \ (q_1),$$

so muß hier wegen jener Voraussetzung das Minuszeichen gelten. Dann folgt aus $-4 = q_1 X^2 - q Y^2$, daß

$$q_1 X^2 \equiv -4, \ (q) \quad \text{oder} \quad X_1^2 \equiv -4q_1, \ (q)$$

ist. D. h. aus $\left(\frac{q}{q_1}\right) = +1$ ergibt sich notwendig $\left(\frac{-q_1}{q}\right) = +1$, oder $\left(\frac{q_1}{q}\right) = -1$, wenn man berücksichtigt, daß $\left(\frac{-1}{q}\right) = -1$ ist.

Wiederholen wir das Resultat dieser letzten Nummer nochmals, so ist gleichzeitig:

$$\left(\frac{q}{q_1}\right) = +1 \quad \text{und} \quad \left(\frac{q_1}{q}\right) = -1,$$

ferner:

$$\left(\frac{q}{q_1}\right) = -1 \quad \text{und} \quad \left(\frac{q_1}{q}\right) = +1,$$

und hiermit ist die Reziprozitätsbeziehung zwischen zwei Primzahlen q_1 und q vollständig gegeben.

Stellt man noch die Fälle 1, 2 und 3 zusammen und bezeichnet nun mit p, q wieder ohne Unterschied beliebige positive, ungerade Primzahlen, so überzeugt man sich schnell, daß das Resultat in folgenden Satz zusammenfaßbar ist:

Satz. *Bedeuten p und q irgendwelche ungerade positive Primzahlen, so gilt für die gegenseitigen Restcharaktere derselben die Gleichung:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Zu diesem Satz treten noch die schon abgeleiteten Sätze über die Restcharaktere von -1 und 2 hinzu als sogenannte *Ergänzungssätze* des Reziprozitätsgesetzes.

1. **Ergänzungssatz.** *Für jede ungerade Primzahl p ist stets:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

2. **Ergänzungssatz.** *Der Restcharakter der Zahl 2 nach irgend einer ungeraden Primzahl p ist:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Diese beiden Ergänzungssätze waren schon Fermat bekannt. Der erste Satz wurde von Euler 1783, der zweite von Lagrange 1775 zum erstenmal bewiesen. (Vergl. P. Bachmann, Niedere Zahlen-

theorie S. 194—195 und S. 196.) Gauß hat den ersten Ergänzungssatz i. J. 1795 entdeckt und er berichtet in der Vorrede zu den Disqu. arithm., daß diese Entdeckung ihn zur tieferen Beschäftigung mit der höheren Arithmetik, also auch zur Aufsuchung und zum Beweis des allgemeinen Reziprozitätsgesetzes geführt hat.

Verwendung des Reziprozitätsgesetzes. Mit Hilfe der gewonnenen Sätze ist es nun leicht, das Symbol $\left(\frac{m}{p}\right)$ für eine beliebige Zahl m und eine Primzahl p auszuwerten.

Um dies zu erläutern, genügen einige Beispiele.

1. $\left(\frac{6}{7}\right)$ soll berechnet werden.

Es ist zuerst, nach der Gleichung $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$:

$$\left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = \left(\frac{3}{7}\right).$$

Nun ist nach dem quadratischen Reziprozitätsgesetz:

$$\left(\frac{3}{7}\right)\left(\frac{7}{3}\right) = -1, \quad \text{also} \quad \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right).$$

Das Symbol $\left(\frac{7}{3}\right)$ vereinfacht man zunächst, indem man 7 durch 1 ersetzt, da $7 \equiv 1$, (3) ist:

$$\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = +1, \quad \text{somit schließlich} \quad \left(\frac{3}{7}\right) = -1,$$

und

$$\left(\frac{6}{7}\right) = -1.$$

2. Welchen Wert hat $\left(\frac{27}{17}\right)$?

Man hat:

$$\left(\frac{27}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) = \left(\frac{5}{17}\right).$$

Nun ist nach dem quadratischen Reziprozitätsgesetz:

$$\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

also

$$\left(\frac{27}{17}\right) = -1.$$

Man könnte dieses Beispiel auch anders durchführen:

$$\left(\frac{27}{17}\right) = \left(\frac{3}{17}\right)^3 \quad \text{usw.}$$

oder

$$\left(\frac{27}{17}\right) = \left(\frac{-7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

Jacobi hat das Reziprozitätsgesetz noch in einer formalen Weise erweitert, welche uns für eine spätere Verwendung nützlich sein wird.

Definiert man nämlich für irgend welche ungerade Primzahlen p q, r ... und irgend eine zu diesen prime Zahl a das Symbol:

$$\left(\frac{a}{p \cdot q \cdot r \ldots}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\left(\frac{a}{r}\right) \ldots,$$

so gilt für eine beliebige zusammengesetzte ungerade Zahl P:

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}},$$

und

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

Ferner gilt für irgend zwei zusammengesetzte relativ prime ungerade Zahlen P, Q:

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Auf den Beweis dieser Formel gehe ich nicht ein, er ist z. B. durch Induktion leicht zu führen, oder auf die aus dem Ansatz:

$$P = [(p-1)+1][(p_1-1)+1]\ldots[(p_\nu-1)+1]$$

folgende Identität:

$$P - 1 = 4a + (p-1) + (p_1-1) + \cdots (p_\nu - 1),$$

in der a eine ganze rationale Zahl bezeichnet, zu gründen.

Man muß aber wieder den allgemeinen Fall und die Ergänzungssätze getrennt behandeln.

26. Darstellung von Zahlen durch Summen von Quadratzahlen.

Aus den bisherigen Tatsachen der Idealtheorie lassen sich einige längst bekannte und berühmte Sätze beweisen, indem man die Zerlegung der Zahlen in speziellen Zahlkörpern untersucht.

I. In Nr. 24, S. 112 ist bewiesen worden, daß im Körper $k(\sqrt{-1})$ jede rationale Primzahl p von der Form $4n+1$ und $p=2$ wesentlich auf *eine* und nur eine einzige Weise in ein Produkt zweier verschiedener Primfaktoren zerlegbar ist in der Form:

$$p = (x + \sqrt{-1}\,y)(x - \sqrt{-1}\,y), \tag{1}$$

da die Faktoren jeder anderen Zerlegung sich von den angeschriebenen Zahlen $x \pm \sqrt{-1}\,y$ nur um Einheitsfaktoren ± 1, $\pm\sqrt{-1}$ unterscheiden können. Anders formuliert besagt die Gleichung (1): Jede

Primzahl p mit der Eigenschaft $p \equiv 1, (4)$ und $p = 2$ läßt sich stets und im wesentlichen nur auf eine einzige Weise in der Form

$$p = x^2 + y^2 \tag{2}$$

darstellen.

Schon Legendre[1]) hat gezeigt, wie man die Zahlenwerte für x, y, welche die Darstellung (2) leisten, durch Entwicklung von $\sqrt{p}$ in einen Kettenbruch, theoretisch berechnen kann. In vielen Fällen erhält man aber auch durch Probieren die gesuchten Zahlen x, y ebenso schnell. Will man nicht einfach die Quadrattafeln, wie sie viele Logarithmentafeln enthalten, benützen, so kann man zuweilen die Zahl der Versuche abkürzen nach der folgenden Überlegung.

Aus der Gleichung (2) folgt eine Kongruenz

$$(zx)^2 + 1 \equiv 0, \ (p),$$

da ja y prim zu p ist. Ist nun w eine Wurzel der Kongruenz

$$X^2 + 1 \equiv 0, \ (p),$$

so ist die gesuchte Zahl x ein Faktor von einer der ganzen Zahlen $w + ap$, der kleiner ist als p oder auch kleiner vorausgesetzt werden kann als $\sqrt{\frac{p}{2}}$, und man braucht dabei für a nur solche ganze Zahlen zu setzen, daß $w + ap$ zwischen $-\frac{p}{2}\sqrt{\frac{p}{2}}$ und $+\frac{p}{2}\sqrt{\frac{p}{2}}$ liegt.

Sind nun p, p_1 zwei ungerade Primzahlen von der Form $4n+1$, so gilt im Körper $k(\sqrt{-1})$ je eine Zerlegung

$$p = (x + \sqrt{-1}\,y)(x - \sqrt{-1}\,y),$$
$$p_1 = (x_1 + \sqrt{-1}\,y_1)(x_1 - \sqrt{-1}\,y_1),$$

und man erhält durch Zusammenfassung der beiden Zerlegungen:

$$pp_1 = (x + \sqrt{-1}\,y)(x - \sqrt{-1}\,y)(x_1 + \sqrt{-1}\,y_1)(x_1 - \sqrt{-1}\,y_1)$$

eine Gleichung, die entweder in der Form

$$pp_1 = (x + \sqrt{-1}\,y)(x_1 + \sqrt{-1}\,y_1)\cdot(x - \sqrt{-1}\,y)(x_1 - \sqrt{-1}\,y_1)$$
$$= \left(xx_1 - yy_1 + (x_1 y + x y_1)\sqrt{-1}\right)\cdot\left(xx_1 - yy_1 - (x_1 y + x y_1)\sqrt{-1}\right),$$
$$pp_1 = (X + \sqrt{-1}\,Y)(X - \sqrt{-1}\,Y) = X^2 + Y^2, \tag{3}$$

oder in der Form

---

1) Zahlentheorie, Bd. I, p. 72. H. Schubert, Auslese aus meiner Unterrichts- und Vorlesungspraxis, Bd. II, p. 178.

$$pp_1 = (x + \sqrt{-1}\,y)(x_1 - \sqrt{-1}\,y_1)\cdot(x - \sqrt{-1}\,y)(x_1 + \sqrt{-1}\,y_1)$$
$$= \left(xx_1 + yy_1 + (x_1y - xy_1)\sqrt{-1}\right)\cdot\left(xx_1 + yy_1 - (x_1y - xy_1)\sqrt{-1}\right),$$
$$pp_1 = (X_1 + \sqrt{-1}\,Y_1)(X_1 - \sqrt{-1}\,Y_1) = X_1^2 + Y_1^2, \qquad (4)$$

so dargestellt werden kann, daß pp_1 als Norm einer ganzen Zahl des Körpers $k(\sqrt{-1})$ erscheint. Das Produkt pp_1 kann daher auf *zwei* wesentlich verschiedene Arten in der Form der Gleichung (3) resp. (4) als Summe zweier Quadratzahlen dargestellt werden.

Wenn $p_1 = 2$ angenommen wird, so ist

$$2p = (1 + \sqrt{-1})(1 - \sqrt{-1})(x + \sqrt{-1}\,y)(x - \sqrt{-1}\,y),$$

und da $1 + \sqrt{-1} = \sqrt{-1}\,(1 - \sqrt{-1})$ ist, so läßt sich $2p$ wieder nur auf eine Weise in eine Summe von Quadraten zerlegen.

Man kann nun dieselben Betrachtungen auf eine beliebige Zahl erweitern und erhält dann, wie der Leser sich selbst überzeugen mag, folgenden von Gauß aufgestellten Satz[1]):

Jede positive ganze rationale Zahl

$$a = 2^e \cdot Q \cdot p_1^{e_1} p_2^{e_2} \ldots p_\nu^{e_\nu},$$

von welcher $p_1, p_2, \ldots p_\nu$ Faktoren von der Form $4n + 1$ zu beliebigen ganzen Exponenten sind und wo Q ein Produkt von Faktoren der Form $4n + 3$ zu geraden Exponenten bedeutet, läßt sich auf verschiedene Weisen als eine Summe von zwei Quadraten

$$a = x^2 + y^2$$

darstellen. Ist einer der Exponenten $e_1, e_2, \ldots e_\nu$ ungerade, so gibt es $E = \frac{1}{2}(e_1 + 1)(e_2 + 1)\ldots(e_\nu + 1)$ und sind alle jene Exponenten gerade $E + \frac{1}{2}$ voneinander verschiedene Darstellungen.

Falls Q aber eine Primzahl von der Form $4n + 3$ zu einer ungeraden Potenz enthält, ist eine Darstellung $a = x^2 + y^2$ überhaupt nicht möglich.

Von diesem Satz ist zuweilen die Umkehrung brauchbar zur Entscheidung darüber, ob eine gegebene Zahl der Form $4n + 1$ Primzahl ist oder nicht.

Anmerkung. Eine sehr interessante und einfache Auflösung der unbestimmten Gleichung

$$p = x^2 + y^2$$

für Primzahlen p hat Gauß gegeben.[2])

---

1) Disquis. arith. V, 182, Anmerkung.

2) Werke, Bd. II, p. 89—91 und in der Selbstanzeige, p. 168.

Wenn $p = 4n + 1$ ist, und x die ungerade, y die gerade Zahl in der verlangten Zerlegung ist, und wenn ferner

$$q = 1 \cdot 2 \ldots n$$
$$r = (n+1)(n+2)\ldots 2n$$

gesetzt wird, so wird $\pm x$ der kleinste Rest (zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$), wenn man $\frac{r}{2q}$ durch p dividiert, und y der kleinste Rest, wenn man $\frac{1}{2}r^2$ durch p dividiert.

Auf den Beweis dieser Behauptung will ich aber hier nicht eingehen.

II. Der Körper $k(\sqrt{-2})$ besitzt nur die Einheiten ± 1 und die Klassenanzahl $h = 1$; es ist die Primzahl $p = 2 = -(\sqrt{-2})^2$, und jede ungerade rationale Primzahl von der Form $8n + 1$, oder $8n + 3$ ist wesentlich nur auf eine einzige Weise in ein Produkt zweier verschiedener Primzahlen zerlegbar in der Weise:

$$p = (x + \sqrt{-2}\,y)(x - \sqrt{-2}\,y).$$

Anders formuliert heißt dies:

Jede positive ungerade Primzahl p von der Form $8n + 1$, oder $8n + 3$ läßt sich auf eine einzige Weise in der Form

$$p = x^2 + 2y^2$$

mit ganzen rationalen Zahlen x, y darstellen.

III. Für den Körper $k(\sqrt{-3})$ ist wieder $h = 1$, und es ist jede Primzahl p wesentlich *eindeutig* zerlegbar, für welche $\left(\frac{-3}{p}\right) = +1$ ausfällt, was allein für die Primzahlen p von der Form $3n + 1$ zutrifft. Ist aber p eine solche Primzahl, so kann die Gleichung

$$p = \left(x + y\frac{1+\sqrt{-3}}{2}\right)\left(x + y\frac{1-\sqrt{-3}}{2}\right)$$

stets auf eine einzige Weise so befriedigt werden, daß x eine ungerade, y eine gerade Zahl wird. Setzt man nämlich

$$p = (a + b\omega)(a + b\omega')$$

und bedenkt, daß a und b nicht beide gerade sein können, weil sonst die rechte Seite durch 4 teilbar wäre und daß, da ± 1, ω, ω' die Einheiten des Körpers sind, auch $p = \omega(a + b\omega)\omega'(a + b\omega')$ usw. gesetzt werden darf, so wird die Bedingung, daß x ungerade und y gerade ausfällt, erfüllt: 1.) für

$$a + b\omega,$$

falls schon a selbst ungerade, b gerade ist; 2.) für

$$(a + b\omega)\,\omega',$$

falls a gerade und b ungerade ist; 3.) für

$$(a + b\omega)\omega = -b + (a + b)\omega,$$

falls a und b ungerade sind. D. h. aber, es gibt für eine Zahl $p \equiv 1, (3)$ eine einzige Zerlegung von der Form:

$$p = \left(x_1 + y_1\sqrt{-3}\right)\left(x_1 - y_1\sqrt{-3}\right),$$

oder:

Jede rationale Primzahl p von der Form $3n + 1$ ist stets und nur auf eine einzige Weise in der Form

$$p = x^2 + 3y^2$$

darstellbar.

Man könnte diese Sätze erweitern auf die Darstellung beliebiger zusammengesetzter Zahlen durch die Formen $x^2 + 2y^2$, $x^2 + 3y^2$, und insbesondere ließen sich noch zahllose weitere Spezialfälle der Darstellung von ganzen Zahlen in der Form $x^2 \pm my^2$ aus der Idealtheorie ableiten, worauf später noch einmal eingegangen wird, Nr. 35 bis 37, doch mögen die angeführten Beispiele genügen, und wir wollen nur noch zeigen, welche Folgerungen aus der Betrachtung der reellen Körper gezogen werden können.

Es möge der Körper $k(\sqrt{2})$ mit der Klassenanzahl $h = 1$ betrachtet werden.

In diesem Körper zerfallen die Primzahlen p von den Formen $8n + 1$ und $8n + 7$. Da jedoch unendlich viele Einheiten im Körper existieren, welche sich durch die Potenzen der Grundeinheit $\varepsilon = 1 + \sqrt{2}$ darstellen lassen, so gehen aus jeder eindeutigen Zerlegung in Primideale

$$(p) = \left(x + y\sqrt{2}\right)\left(x - y\sqrt{2}\right)$$

unendlich viele Darstellungen der Zahl $\pm p$ in der Form $x^2 - 2y^2$ hervor.

Wenn nämlich $p = x^2 - 2y^2$ ist, so ist auch

$$-p = (x + 2y)^2 - 2(x + y)^2,$$

oder

$$-p = (x - 2y)^2 - 2(x - y)^2,$$

da

$$-p = \left(x + y\sqrt{2}\right)\varepsilon \cdot \left(x - y\sqrt{2}\right)\varepsilon' \text{ ist, usw.}$$

Analog wird, wegen:

$$p = \left(x + y\sqrt{2}\right)\varepsilon^2\left(x - y\sqrt{2}\right)\varepsilon'^2,$$

$$p = (3x + 4y)^2 - 2(2x + 3y)^2.$$

Man hat also den Satz:

Jede positive oder negative Primzahl, die positiv genommen von der Form $8n \pm 1$ *ist, läßt sich auf unendlich viele verschiedene Weisen in der Form*

$$x^2 - 2y^2$$

darstellen, und zwar lassen sich alle Darstellungen aus einer einzigen unter Verwendung der Einheiten $\pm \varepsilon^e$ *des Körpers ableiten.*

Auch diesem Satze können zahllose andere derselben oder ähnlicher Art an die Seite gestellt werden.

27. Hilberts Normenrestsymbol.

Wir wenden uns nun zu einer neuen, ziemlich weitläufigen Untersuchung, nämlich zu einer Einteilung der Idealklassen in Geschlechter.

Es handelt sich hierbei um eine Klassifikation, welche der Theorie der quadratischen Formen entnommen ist, wo sie von Gauß zum erstenmal ausgeführt wurde. (S. Disquis. arithm. V, Art. 231ff.) Gauß hat diesem Gegenstand einen großen Teil der sect. V der Disquis. arithm. gewidmet, indem er selbst die Sätze über die Geschlechter zu den schönsten und schwierigsten Untersuchungen der höheren Arithmetik rechnet.

Der Einteilung der Klassen in Geschlechter entspringt ein neuer Beweis des quadratischen Reziprozitätsgesetzes, der insofern einen großen Vorzug vor allen anderen Beweisen dieses Satzes hat, als er sich auch verallgemeinern läßt für die höheren Reziprozitätsgesetze.

Wegen der großen Bedeutung, welche daher die Einteilung der Klassen in Geschlechter besitzt, erscheint es mir notwendig, auch hier die entsprechenden Fragen zu erörtern, und zwar ist das sehr wohl möglich, da Herr Hilbert[1]) für den quadratischen Zahlkörper die Darstellung ungemein vereinfacht und ihr eine Form gegeben hat, welche wohl lange endgültig bleiben wird.

Diese vereinfachte Darstellung ist ganz wesentlich erst ermöglicht worden durch die Einführung eines neuen Symbols, das zunächst hier erklärt werden muß.

Definition. Es bedeute p eine positive rationale Primzahl und m, n zwei beliebige ganze rationale Zahlen, nur soll m keine quadratischen Faktoren enthalten.

Wenn alsdann für jede beliebige positive ganzzahlige Potenz p^e

1) Vergl. Zahlbericht, Kap. XVII, § 64—66, 70 und Kap. XVIII, § 71—78.

von p die Zahl n kongruent ist der Norm einer ganzen Zahl α des Körpers $k(\sqrt{m})$ nach dem Modul p^e, wenn also $n \equiv n(\alpha)$, (p^e) ausfällt für jede ganze rationale positive Zahl e, so setze man

$$\left(\frac{n,\, m}{p}\right) = +1.$$

Wenn dagegen keine Zahl α im Körper $k(\sqrt{m})$ gefunden werden kann, so daß $n \equiv n(\alpha)$, (p) ist, oder wenn die Kongruenz $n \equiv n(\alpha)$, (p^e) nicht für alle positiven ganzzahligen Werte von e durch ganze Zahlen α des Körpers erfüllbar ist, so sei

$$\left(\frac{n,\, m}{p}\right) = -1.$$

Im ersten Fall heißt die Zahl n ein **Normenrest**, im zweiten Fall ein **Normennichtrest** des Körpers $k(\sqrt{m})$ nach dem Modul p.

Ein wesentlicher Grund für die Brauchbarkeit des Symbols liegt darin, daß sich für dasselbe einfache Rechnungsregeln, ähnlich wie sie für das Legendresche Symbol existieren, nachweisen lassen.

Der Entwicklung dieser Regeln sollen einige allgemeine Bemerkungen vorausgeschickt werden.

1.) Man kann n stets als eine ganze Zahl ohne quadratischen Faktor voraussetzen; denn, wenn $n = a^2 n_1$ ist, so wird:

$$\left(\frac{n,\, m}{p}\right) = \left(\frac{n_1,\, m}{p}\right).$$

2.) Von den sämtlichen nach p einander inkongruenten Zahlen eines Restsystems $1, \ldots p-1$ sind die Hälfte quadratische Reste und die übrigen quadratische Nichtreste nach p. Bezeichnen

$$r_1,\ r_2,\ \ldots\ r_{\frac{p-1}{2}}$$

die quadratischen Reste nach p und

$$n_1,\ n_2,\ \ldots\ n_{\frac{p-1}{2}}$$

die quadratischen Nichtreste, und bedeutet ferner n einen beliebigen Nichtrest, so ist unter den Differenzen:

$$d_1 = r_1 - n,\ d_2 = r_2 - n,\ \ldots\ d_{\frac{p-1}{2}} = r_{\frac{p-1}{2}} - n$$

wenigstens ein *Nichtrest* nach p enthalten.

Die Behauptung ist offenbar richtig für $p = 3$.

Ist p eine Primzahl > 3, so zeigt man zunächst, daß keine zwei der Zahlen d_ν einander nach p kongruent sein können.

Daraus folgt aber, daß auch nicht zwei der Zahlen d_ν einem und demselben Rest kongruent sein können.

Angenommen nun, die sämtlichen Zahlen $d_1, d_2 \ldots$ wären quadratische Reste, so wäre

$$d_1 \equiv r_{k_1}, \ (p),$$

oder

$$r_1 - n \equiv r_{k_1}, \ (p),$$

resp.

$$n \equiv r_1 - r_{k_1}, \ (p)$$

und desgl.:

$$n \equiv r_2 - r_{k_2}, \ (p)$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$n \equiv r_i - r_{k_i}, \ (p)$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$n \equiv r_{\frac{p-1}{2}} - r_{k_{\frac{p-1}{2}}}, \ (p),$$

wo die Zahlen $r_{k_1}, r_{k_2}, \ldots r_{k_{\frac{p-1}{2}}}$ mit den Zahlen $r_1, \ldots r_{\frac{p-1}{2}}$ in anderer, nicht bekannter Reihenfolge übereinstimmen. Durch Addition aller dieser Kongruenzen erhält man daher rechts 0, es folgt also aus der Annahme über die Größen d:

$$\frac{p-1}{2} \cdot n \equiv 0, \ (p);$$

aber diese Kongruenz kann nicht bestehen, da sowohl $\frac{p-1}{2}$ als auch n zu p prim sind. Es muß sich mithin unter den Differenzen d mindestens ein Nichtrest befinden.

Berücksichtigt man noch, daß für $p > 3$, den Fall $p = 3$ also ausgenommen:

$$\sum_1^{\frac{p-1}{2}} r_i \ \text{ und } \ \sum_1^{\frac{p-1}{2}} n_i \equiv 0, \ (p)$$

sind, so folgt andererseits auch, daß unter den Zahlen d_i mindestens ein Rest sich befinden muß.

Bezeichnet ferner r einen beliebigen Rest, d. h. eine der Zahlen r_i, so läßt sich weiter auf ähnliche Weise zeigen, daß in den Differenzenreihen

$$n_i - r, \quad r_i \pm r, \quad n_i \pm n$$

stets Reste und Nichtreste vorkommen.

Den Rechnungsregeln für das Hilbertsche Symbol liegen Eigenschaften dieses Symbols zugrunde, die in den vier folgenden Sätzen entwickelt werden sollen.

1. Satz. *Wenn n, m zwei ganze rationale Zahlen sind und p eine ungerade Primzahl bezeichnet, welche in n und in m nicht aufgeht, so ist stets:*

A.) $$\left(\frac{n,\, m}{p}\right) = +1,$$

B.) $$\left(\frac{n,\, p}{p}\right) = \left(\frac{p,\, n}{p}\right) = \left(\frac{n}{p}\right).$$

Wenn ferner sowohl n als auch m nur durch die erste Potenz der ungeraden Primzahl p teilbar ist, so ist:

C.) $$\left(\frac{n,\, m}{p}\right) = \left(\frac{-\frac{n\,m}{p^2}}{p}\right).$$

Beweis A.) Es sei zunächst
$$m \not\equiv 1,\ (4)\ \ (\text{also } m \equiv 2,\ 3,\ (4)),$$
so behauptet der Satz *erstens*, daß die Kongruenz:
$$n \equiv x^2 - my^2,\ (p),$$
oder
$$x^2 - my^2 - n \equiv 0,\ (p), \tag{1}$$
stets durch ganze rationale Zahlen x, y lösbar ist.

In der Tat, ist $\left(\frac{n}{p}\right) = +1$, $\left(\frac{m}{p}\right) = \pm 1$, so ist die Kongruenz (1) dadurch zu befriedigen, daß man $y \equiv 0$ annimmt und für x irgend eine Lösung der Kongruenz
$$x^2 - n \equiv 0,\ (p)$$
setzt.

Ist ferner $\left(\frac{m}{p}\right) = +1$, $\left(\frac{n}{p}\right) = \pm 1$, so kann $m \equiv z^2$, (p) gesetzt und die Kongruenz (1) folgendermaßen geschrieben werden:
$$x^2 - z^2y^2 - n \equiv 0,\ (p). \tag{2}$$
Da n nach dem Modul p stets einer *ungeraden* Zahl kongruent ist, kann man für x und zy unmittelbar setzen:
$$x \equiv \frac{n+1}{2},\ (p) \tag{3}$$
$$zy \equiv \frac{n-1}{2},\ (p). \tag{4}$$

Nun läßt sich die Kongruenz (4) offenbar immer durch eine ganze Zahl y befriedigen, weil z prim zu p ist, folglich ist auch die Kongruenz (1) durch ganze Zahlen x, y lösbar.

Ist schließlich $\left(\frac{n}{p}\right) = -1$ und $\left(\frac{m}{p}\right) = -1$, dann durchläuft das Produkt my^2 für die Zahlen $y = 1, \ldots p-1$ alle Nichtreste nach p zweimal. Wenn man andererseits statt x^2 die sämtlichen Reste nach p einführt, so muß unter den Zahlen $x^2 - n$ ebenfalls mindestens ein Nichtrest sein, also läßt auch die Kongruenz (1) mindestens ein ganzzahliges Lösungssystem x, y zu.

Damit ist nun bewiesen, daß unter den Voraussetzungen des Satzes die Kongruenz (1) immer lösbar ist. Es ist der erste Schritt getan zum Beweise der Formel A) für den Fall, daß $m \not\equiv 1$, (4) ist.

Es sei jetzt andererseits $m \equiv 1$, (4), so ist die Grundbedingung für die Richtigkeit des Satzes die, daß die Kongruenz:

$$n \equiv \left(x + \frac{y}{2}\right)^2 - \frac{m}{4} y^2, \ (p),$$

oder die ihr gleichwertige Kongruenz:

$$4n \equiv (2x + y)^2 - my^2, \ (p) \tag{1a}$$

lösbar ist. Es ist klar, daß hier genau dieselben Betrachtungen gelten, wie sie eben angestellt worden sind.

Nachdem so nachgewiesen ist, daß für die erste Potenz von p stets eine ganze Zahl α des Körpers existiert von der Beschaffenheit, daß

$$n \equiv n(\alpha), \ (p)$$

wird, fehlt *zweitens* noch der Nachweis, daß auch zu einer beliebigen Potenz p^e von p jedesmal eine ganze Zahl α existiert, für welche: $n \equiv n(\alpha)$, (p^e) ausfällt.

Dieser Nachweis wird geführt durch den Schluß von $e-1$ auf e.

Angenommen, es sei $\alpha_1 = a + b\omega$ eine ganze Zahl des Körpers $k(\sqrt{m})$, für welche die Kongruenz $n \equiv n(\alpha_1)$, (p^{e-1}) erfüllt ist, so setzt man $x = a + up^{e-1}$, $y = b + vp^{e-1}$ und bestimmt zwei ganze Zahlen u, v derart, daß:

$$n \equiv n(x + y\omega), \ (p^e)$$

wird. Für den Fall $m \not\equiv 1$, (4) z. B. erhält man zur Berechnung von u, v eine Kongruenz:

$$2au - 2bv - \frac{a^2 - b^2 m - n}{p^{e-1}} \equiv 0, \ (p).$$

Dieselbe ist stets lösbar, da a und b nicht beide durch p teilbar sein können. Wenn also eine ganze Zahl α_1 existiert, so daß $n \equiv n(\alpha_1)$, (p^{e-1}) wird, so kann man hieraus x, y stets so berechnen, daß die

weitere Kongruenz $n \equiv n(x + y\omega)$, (p^e) erfüllt ist. Ganz ähnlich verhält es sich im Falle $m \equiv 1$, (4).

Die Kongruenz $n \equiv n(x + y\omega)$, (p^e) läßt sich aber befriedigen für $e = 1$, also auch für $e = 2, 3, \ldots$, und somit ist allgemein:

$$\left(\frac{n,\, m}{p}\right) = +1,$$

womit die erste Behauptung des Satzes bewiesen ist.

B.) Wenn $m = p$ ist, so sind die Kongruenzen:

$$x^2 - py^2 - n \equiv 0,\ (p^e),\ \text{falls } p \not\equiv 1,\ (4) \text{ ist,} \tag{5}$$

resp.

$$(2x + y)^2 - py^2 - 4n \equiv 0,\ (p^e),\ \text{falls } p \equiv 1,\ (4) \text{ ist,} \tag{6}$$

dann und nur dann für alle ganzen positiven Exponenten e lösbar, wenn $\left(\frac{n}{p}\right) = +1$ ausfällt, und unlösbar, wenn $\left(\frac{n}{p}\right) = -1$ ist. Falls schließlich $n = p$ ist, so sind die Kongruenzen $x^2 - my^2 - p \equiv 0$, (p^e) usw. stets dann und nur dann lösbar, wenn schon

$$x^2 - my^2 \equiv 0,\ (p)$$

lösbar ist, oder wenn $\left(\frac{m}{p}\right) = +1$ ausfällt; also ist, wie es der Satz behauptet,

$$\left(\frac{n,\, p}{p}\right) = \left(\frac{p,\, n}{p}\right) = \left(\frac{n}{p}\right).$$

Diese letzte Gleichung läßt sich unmittelbar erweitern auf den Fall, daß n *oder* m durch p^1 teilbar ist; man findet:

$$\left(\frac{pn_1,\, m}{p}\right) = \left(\frac{m,\, pn_1}{p}\right) = \left(\frac{m}{p}\right).$$

C.) Ist endlich sowohl m als auch n durch die erste Potenz von p, aber nicht durch p^2 teilbar ($m = pm_1$ und $n = pn_1$), so sind die in Frage kommenden Kongruenzen:

$$x^2 - my^2 - n \equiv 0,\ (p^e),$$

resp.

$$(2x + y)^2 - my^2 - 4n \equiv 0,\ (p^e)$$

stets und nur dann lösbar, wenn auch schon eine Kongruenz von der Form

$$pX^2 - m_1 Y^2 - n_1 \equiv 0,\ (p)$$

lösbar ist. Hierzu ist notwendig und hinreichend, daß:

$$m_1 Y^2 + n_1 \equiv 0,\ (p),$$

oder

$$(m_1 Y)^2 + m_1 n_1 \equiv 0,\ (p),$$

lösbar ist, daß also $\left(\frac{-m_1 n_1}{p}\right) = +1$ wird. D. h. aber, es ist:

$$\left(\frac{n,\, m}{p}\right) = \left(\frac{-\frac{n \cdot m}{p^2}}{p}\right),$$

somit ist der 1. Satz vollständig bewiesen.

2. Satz. *Wenn m, n zwei ganze rationale ungerade Zahlen sind, so gelten die Gleichungen:*

$$\text{A.)} \qquad \left(\frac{n,\, m}{2}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}$$

und

$$\text{B.)} \qquad \left(\frac{n,\, 2}{2}\right) = \left(\frac{2,\, n}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Beweis. In dem Beweis für die Formel A.) handelt es sich um den Nachweis der Existenz von Lösungen der Kongruenzen:

$$x^2 - my^2 - n \equiv 0,\ (2^e),\ \text{wenn } m \not\equiv 1,\ (4) \text{ ist}, \tag{1}$$

resp.

$$x^2 + xy + \frac{1-m}{4}y^2 - n \equiv 0,\ (2^e),\ \text{wenn } m \equiv 1,\ (4) \text{ ist}, \tag{2}$$

und in dem Beweis für die Formel B.) um den entsprechenden Nachweis bezüglich der Kongruenzen:

$$x^2 - 2y^2 - n \equiv 0,\ (2^e), \tag{3}$$

und

$$x^2 - ny^2 - 2 \equiv 0,\ (2^e) \tag{4}$$

$$\text{resp. } x^2 + xy + \frac{1-n}{4}y^2 - 2 \equiv 0,\ (2^e), \tag{5}$$

je nachdem in den beiden letzten Fällen $n \not\equiv 1$, oder $n \equiv 1$, (4) ist.

Man erkennt zunächst leicht, daß diese Kongruenzen für $e = 1$ alle lösbar sind, daß aber die Lösbarkeit für diesen Fall noch nicht hinreicht als Bedingung für die Lösbarkeit in den Fällen $e > 2$. Wir wollen nun zeigen, daß die Kongruenzen dann für alle Exponenten e lösbar sind, wenn sie für $e = 3$ gelöst werden können.

Vorausgesetzt, $x = a$, $y = b$ sei eine Lösung der Kongruenz:

$$x^2 - my^2 - n \equiv 0,\ (2^3), \tag{1), (3), (4}$$

(indem wir hier die Kongruenzen (1), (3), (4) in naheliegender Weise zusammenfassen), und es sei außerdem der Ausdruck $a^2 - mb^2 - n$ nicht mehr durch 2^4 teilbar, so setzt man:

$$x = a + 2^2u, \quad y = b + 2^2v,$$

dann wird

$$x^2 - my^2 - n = a^2 - mb^2 - n + 8\,(au - mbv) + 16\,(u^2 - mv^2),$$

und man erhält daher:

$$x^2 - my^2 - n \equiv 0, \ (2^4),$$

wenn die Kongruenz:

$$\frac{a^2 - mb^2 - n}{8} + au - mbv \equiv 0, \ (2),$$

oder:

$$au - mbv + 1 \equiv 0, \ (2) \qquad (6)$$

befriedigt werden kann.

Nun ergibt sich aus der Kongruenz (1) der Wert von a oder b und aus den Kongruenzen (3), (4) der Wert von a ungerade, daher ist die Kongruenz (6) lösbar. In ähnlicher Weise schließt man nun weiter von der Lösbarkeit der Kongruenz: $x^2 - my^2 - n \equiv 0, \ (2^e)$, für $e = 4$ auf die Lösbarkeit für $e = 5, 6 \ldots e$. Bei dieser Erweiterung verlangt der Fall der Kongruenz (3), mit $m = 2$, eine kleine Änderung in dem Ansatz für x, y, wie man sich leicht überzeugt.

Durch die gleiche Schlußweise, wie sie eben für die Kongruenzen (1), (3), (4) angewendet wurde, zeigt man auch, daß die Kongruenzen (2) resp. (5) für *jeden* Exponenten e erfüllbar sind, falls sie schon für $e = 3$ befriedigt werden können. Wenn $x = a$, $y = b$ eine Lösung dieser Kongruenzen für $e = 3$ ist, so hat man zur Bestimmung der Lösung für $e = 4$:

$$x = a + 8u, \quad y = b + 8v$$

zu setzen und alsdann u, v derart zu bestimmen, daß:

$$x^2 + xy + \frac{1 - m}{4} y^2 - n \equiv 0, \ (2^4)$$

resp.

$$x^2 + xy + \frac{1 - n}{4} y^2 - 2 \equiv 0, \ (2^4)$$

wird. Dazu ist aber eine Kongruenz zu lösen von der Form:

$$av + bu + 1 \equiv 0, \ (2),$$

und diese Kongruenz ist stets lösbar, da im Fall der Kongruenz (2) der Wert a oder b und im Falle der Kongruenz (5) sicher b ungerade sein muß; usw.

Um nun vollends zu entscheiden, für welche Werte m, n die Kongruenzen (1) bis (5) zu jedem Exponenten e lösbar sind, genügt es daher, wenn man in den Kongruenzen:

$$x^2 - my^2 - n \equiv 0, \ (8),$$

resp.

$$x^2 + xy + \frac{1 - m}{4} y^2 - n \equiv 0, \ (8)$$

für m und n alle Kombinationen der Zahlen 1, 2, 3, 5, 7 durchprobiert. (Vgl. übrigens hierzu noch den Beweis von Satz 3.) Um jedoch

gleich eine für den nachfolgenden Satz notwendige Tatsache abzuleiten, ist es zweckmäßig, auch noch $m, n = 6$ zu setzen. Man erhält alsdann die folgende Tabelle, welche so angeordnet ist, daß in der ersten Spalte die Zahlen m von 1 bis 7 aufgeschrieben sind, und in der zweiten Spalte diejenigen Werte n von 1 bis 7, für welche die entsprechende Kongruenz unter (1) bis (5) lösbar ist.

m	n
1	1, 2, 3, 5, 6, 7
2	1, 2, 7
3	1, 5, 6
5	1, 3, 5, 7
6	1, 3, 6
7	1, 2, 5

Aus dieser Tabelle bestätigt man, daß für ein ungerades n und ein ungerades m:

A.) $$\left(\frac{n,\ m}{2}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$$

ist. Ferner wird für ein ungerades n:

$$\left(\frac{2,\ n}{2}\right) = \left(\frac{n,\ 2}{2}\right) = +1 \text{ oder } -1,$$

je nachdem $n \equiv \pm 1, (8)$, oder $n \equiv \pm 3, (8)$ ist. Man kann dieses Resultat in der Formel ausdrücken:

B.) $$\left(\frac{2,\ n}{2}\right) = \left(\frac{n,\ 2}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Die eben aufgestellte Tabelle mag gleich benutzt werden zur Diskussion der Fälle, wo $p = 2$ ist und m oder n bezw. m und n gerade Zahlen sind.

3. Satz. *Wenn m, n, m_1, n_1 ganze rationale ungerade Zahlen sind, so ist:*

A.) $$\left(\frac{n,\ 2m_1}{2}\right) = \left(\frac{n,\ 2}{2}\right)\left(\frac{n,\ m_1}{2}\right)$$

B.) $$\left(\frac{2n_1,\ m}{2}\right) = \left(\frac{2,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right)$$

C.) $$\left(\frac{2n_1,\ 2m_1}{2}\right) = \left(\frac{-m_1 n_1,\ 2m_1}{2}\right).$$

Beweis A.) Man erkennt vorerst wieder auf ähnliche Weise wie beim vorhergehenden Satze, daß die Kongruenz:

$$x^2 - 2m_1 y^2 - n \equiv 0, \ (2^e)$$

stets und nur dann erfüllbar ist, wenn sie für $e = 3$ bestehen kann. Es genügt daher für $2m_1$ und n, die Zahlen in der angeschriebenen Tabelle zu nnehmen. Man verifiziert danach leicht die Gültigkeit der Gleichung:

$$\left(\frac{n,\ 2m_1}{2}\right) = (-1)^{\frac{n^2-1}{8} + \frac{n-1}{2} \cdot \frac{m_1-1}{2}},$$

oder es ist wirklich:

A.) $$\left(\frac{n,\ 2m_1}{2}\right) = \left(\frac{n,\ 2}{2}\right)\left(\frac{n,\ m_1}{2}\right).$$

Denn es ist $\left(\frac{n,\ 2m_1}{2}\right) = +1$, wenn $m_1 \equiv 1, (8)$ und $n \equiv \pm 1, (8)$ ist, oder wenn $m_1 \equiv 3, (4)$ und $n \equiv 1, (8)$ bezw. $n \equiv 3, (8)$ ist.

B.) Um den Wert des Symbols $\left(\frac{2n_1,\ m}{2}\right)$ zu bestimmen, hat man die zwei Fälle zu unterscheiden: $m \equiv 3, (4)$ und $m \equiv 1, (4)$.

B, 1.) $m \equiv 3, (4)$. Das Hilbertsche Symbol hat den Wert $+1$, wenn die Kongruenz

$$x^2 - my^2 - 2n_1 \equiv 0, \ (2^e)$$

für alle Exponenten e lösbar ist. Dies ist auch hier wiederum der Fall, wenn die Kongruenz für $e = 3$ durch ganze rationale Zahlen befriedigt werden kann, da die Kongruenz gegebenenfalls sicher nur durch ungerade Werte x, y zu lösen ist.

Aus der Tabelle ergibt sich nun:

$$\left(\frac{2n_1,\ m}{2}\right) = +1,$$

wenn $n_1 \equiv 1, (4)$ und $m \equiv \pm 1, (8)$ ist, oder wenn $n_1 \equiv 3, (4)$ und $m \equiv 1, (8)$ oder $m \equiv 3, (8)$ ist; diese Formeln zusammen mit den Werten, für welche $\left(\frac{2n_1,\ m}{2}\right) = -1$ ausfällt, lassen sich vereinigen zu dem Ausdruck:

$$\left(\frac{2n_1,\ m}{2}\right) = (-1)^{\frac{m^2-1}{8} + \frac{n_1-1}{2} \cdot \frac{m-1}{2}},$$

oder es ist:

$$\left(\frac{2n_1,\ m}{2}\right) = \left(\frac{2,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right).$$

B, 2.) $m \equiv 1, (4)$. Unter dieser Voraussetzung ist zu untersuchen, ob die Kongruenz:

$$x^2 + xy + \frac{1-m}{4} y^2 - 2n_1 \equiv 0, \ (2^e), \tag{1}$$

oder auch:

$$(2x+y)^2 - my^2 - 8n_1 \equiv 0,\ (2^{e+2}) \tag{1a}$$

auflösbar ist; diese Kongruenz kann man schreiben:

$$X^2 - mY^2 - 8n_1 \equiv 0,\ (2^{e_1}). \tag{2}$$

Die letzte Kongruenz ist stets lösbar für $e_1 = 2$; sie ist ferner lösbar für $e_1 = 3$, wenn

$$X^2 - mY^2 \equiv 0,\ (8) \tag{2a}$$

durch ganze rationale Zahlen befriedigt werden kann. Umgekehrt ist aber die Kongruenz (2) für $e_1 = 4$ und $e_1 > 4$ nur lösbar, wenn X, Y solche ganze Zahlen sind, daß zwar

$$X^2 - mY^2 \equiv 0,\ (8),\quad \text{aber nicht}\quad X^2 - mY^2 \equiv 0,\ (16)$$

ausfällt. D. h. X, Y dürfen *keine geraden* Zahlen sein, und daraus folgt, daß die Kongruenz (2a) nur noch für $m \equiv 1$, (8) Lösungen besitzt. Es gibt insbesondere dann zwei ganze rationale Zahlen x, y, welche die ursprüngliche Kongruenz (1) befriedigen. Wie in den vorausgehenden Fällen folgt nun weiter, daß die Kongruenz (2) für jedes e_1 bezw. (1) für jedes e lösbar ist, falls die Bedingung $m \equiv 1$, (8) erfüllt ist. Auf die Beschaffenheit von n_1 kommt es für den vorliegenden Fall nicht an; man erhält einfach:

$$\left(\frac{2n_1,\ m}{2}\right) = +1,\ \text{wenn}\ m \equiv 1,\ (8),$$

$$\left(\frac{2n_1,\ m}{2}\right) = -1,\ \text{wenn}\ m \equiv 5,\ (8)\ \text{ist},$$

oder es ist unter Berücksichtigung der bisherigen Resultate, und wegen $m \equiv 1$, (4):

$$\left(\frac{2n_1,\ m}{2}\right) = (-1)^{\frac{m^2-1}{8}} = \left(\frac{2,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right).$$

Faßt man nun die beiden Möglichkeiten $m \equiv 1$, $m \equiv 3$, (4) zusammen, so ist beide Mal:

B.) $$\left(\frac{2n_1,\ m}{2}\right) = \left(\frac{2,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right).$$

C.) Der Wert des Symbols $\left(\frac{2n_1,\ 2m_1}{2}\right)$ hängt ab von den Eigenschaften der Kongruenz:

$$x^2 - 2m_1y^2 - 2n_1 \equiv 0,\ (2^e). \tag{1}$$

Diese Kongruenz ist lösbar für alle Werte von e, für welche auch die Kongruenz

$$2m_1x^2 - (2m_1y)^2 - 4m_1n_1 \equiv 0,\ (2^{e+1}) \tag{1a}$$

lösbar ist. Hieraus ergeben sich aber x und $2m_1y$ stets gerade; sub-

stituiert man daher: $x = 2X$, $m_1 y = Y$, und dividiert die ganze Kongruenz durch 4, so erhält man anstelle der Kongruenz (1) die folgende:

$$Y^2 - 2m_1 X^2 + m_1 n_1 \equiv 0, \ (2^{e-1}). \qquad (1\text{b})$$

Nun entspricht jeder Lösung der Kongruenz (1) eine Lösung von (1b) und umgekehrt.

Daher ist:

$$\left(\frac{2n_1, 2m_1}{2}\right) = \left(\frac{-m_1 n_1, 2m_1}{2}\right),$$

womit jetzt alle drei Formeln des Satzes bewiesen sind.

4. Satz. *Wenn m, n, m_1, n_1 beliebige ganze rationale Zahlen ohne quadratische Faktoren sind und wenn p eine rationale Primzahl bedeutet, so gelten die Gleichungen:*

A.) $$\left(\frac{-m, m}{p}\right) = +1$$

B.) $$\left(\frac{n, m}{p}\right) = \left(\frac{m, n}{p}\right)$$

C.) $$\left(\frac{nn_1, m}{p}\right) = \left(\frac{n, m}{p}\right)\left(\frac{n_1, m}{p}\right)$$

D.) $$\left(\frac{n, mm_1}{p}\right) = \left(\frac{n, m}{p}\right)\left(\frac{n, m_1}{p}\right).$$

Beweis A.) Die Gleichung A.) ist selbstverständlich richtig, da $-m$ die Norm von $\sqrt{m}$ ist und daher für jede Zahl p die Kongruenz:

$$-m \equiv n(\sqrt{m}), \ (p^e)$$

gilt.

B.) Die Formel B.) gilt *erstens* für ein ungerades p. Denn wenn n und m zu p prim sind, so ist $\left(\frac{n, m}{p}\right) = \left(\frac{m, n}{p}\right) = 1$. Ist aber n oder m durch p teilbar, so ist:

$$\left(\frac{pn_1, m}{p}\right) = \left(\frac{m}{p}\right), \quad \left(\frac{m, pn_1}{p}\right) = \left(\frac{m}{p}\right)$$

und

$$\left(\frac{n, pm_1}{p}\right) = \left(\frac{n}{p}\right), \quad \left(\frac{pm_1, n}{p}\right) = \left(\frac{n}{p}\right);$$

wenn schließlich m und n durch p^1 teilbar sind, so ist:

$$\left(\frac{m, n}{p}\right) = \left(\frac{n, m}{p}\right) = \left(\frac{-\frac{mn}{p^2}}{p}\right).$$

Zweitens gilt die Formel B.) auch für $p = 2$. Aus dem dritten Satz folgt dies unmittelbar für die Fälle, wo mindestens eine der beiden Zahlen m, n ungerade ist. Sind aber beide Zahlen m und n gerade, so ist:

$$\left(\frac{n,\ m}{2}\right)=\left(\frac{2n_1,\ 2m_1}{2}\right)=\left(\frac{-m_1n_1,\ 2m_1}{2}\right)=\left(\frac{-m_1n_1,\ 2}{2}\right)\left(\frac{-m_1n_1,\ m_1}{2}\right)$$

und

$$\left(\frac{m,\ n}{2}\right)=\left(\frac{-m_1n_1,\ 2}{2}\right)\left(\frac{-m_1n_1,\ n_1}{2}\right).$$

Da nun:

$$\left(\frac{-m_1n_1,\ n_1}{2}\right)=(-1)^{\frac{-m_1n_1-1}{2}\cdot\frac{n_1-1}{2}}$$

und

$$\left(\frac{-m_1n_1,\ m_1}{2}\right)=(-1)^{\frac{-m_1n_1-1}{2}\cdot\frac{m_1-1}{2}}$$

ist, und da stets (wie man durch Einsetzen der Werte $m_1\equiv\pm 1$, $n_1\equiv\pm 1, (4)$ erkennt):

$$\frac{-m_1n_1-1}{2}\cdot\frac{m_1-n_1}{2}\equiv 0,\ (2)$$

ausfällt, so gilt die Formel B.) auch für $p=2$, folglich ist sie ganz allgemein gültig.

C.) Die Formel C.) gilt zunächst wieder für ein ungerades p. Falls nämlich nn_1 prim ist zu p, so hat man entweder:

$$\left(\frac{nn_1,\ m}{p}\right)=1=\left(\frac{n,\ m}{p}\right)\left(\frac{n_1,\ m}{p}\right),$$

falls nämlich auch m durch p nicht teilbar ist, oder:

$$\left(\frac{nn_1,\ pm_1}{p}\right)\equiv\left(\frac{nn_1}{p}\right)=\left(\frac{n}{p}\right)\left(\frac{n_1}{p}\right)=\left(\frac{n,\ pm_1}{p}\right)\left(\frac{n_1,\ pm_1}{p}\right)$$

für $m=pm_1$. Analog verhält sich die Formel, wenn nn_1 durch p teilbar ist.

Nimmt man $p=2$, so folgt die Formel C.) aus dem dritten Satz, und aus der Tatsache, daß für *ungerade* $m,\ n,\ n_1$:

$$\left(\frac{nn_1,\ m}{2}\right)=\left(\frac{n,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right)$$

und

$$\left(\frac{nn_1,\ 2}{2}\right)=\left(\frac{n,\ 2}{2}\right)\left(\frac{n_1,\ 2}{2}\right)$$

ist, wie man leicht beweist. In der Tat ist:

$$\left(\frac{n,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right)=(-1)^{\frac{m-1}{2}\left(\frac{n-1}{2}+\frac{n_1-1}{2}\right)};$$

wegen der Voraussetzung über $n,\ n_1$ ist aber:

$$\frac{n-1\cdot n_1-1}{2}\equiv 0,\ (2),$$

daher gilt die Kongruenz:

$$\frac{n-1}{2}+\frac{n_1-1}{2}\equiv\frac{nn_1-1}{2},\ (2),$$

und hieraus folgt:

$$\left(\frac{n,\ m}{2}\right)\left(\frac{n_1,\ m}{2}\right)=\left(\frac{nn_1,\ m}{2}\right).$$

Die Gleichung:

$$\left(\frac{nn_1,\ 2}{2}\right)=\left(\frac{n,\ 2}{2}\right)\left(\frac{n_1,\ 2}{2}\right),$$

ergibt sich durch direkte Berechnung, wenn man noch bedenkt, daß die Kongruenz besteht:

$$\frac{n^2 n_1^2-1}{8}\equiv\frac{n^2-1}{8}+\frac{n_1^2-1}{8},\ (2).$$

D.) Die Formel D.) endlich beweist man, indem man, von dem Symbol $\left(\frac{n,\ mm_1}{p}\right)$ ausgehend, zuerst die Formel B.), dann die Formel C.) und schließlich auf jeden Faktor nochmals die Formel B.) dieses Satzes anwendet.

Berücksichtigt man noch, daß $\left(\frac{n,\ m}{p}\right)=+1$ ist für jede Primzahl p, wenn n die Norm einer ganzen Zahl α des Körpers $k(\sqrt{m})$ ist, so ergibt sich insbesondere aus dem 4. Satz auch die Gleichung:

$$\left(\frac{n\cdot n(\alpha),\ m}{p}\right)=\left(\frac{n,\ m}{p}\right).$$

28. Das Charakterensystem eines Ideals.

Wenn a eine ganze rationale Zahl ist, und wenn ferner $l_1,\ l_2 \ldots l_t$ die voneinander verschiedenen rationalen Primzahlen bezeichnen, welche in der Diskriminante d eines Körpers $k(\sqrt{m})$ aufgehen, dann nennt man nach dem Vorgang von Gauß die Gesamtheit der t Einheiten ± 1:

$$\left(\frac{a,\ m}{l_1}\right),\ \left(\frac{a,\ m}{l_2}\right)\ \cdots\ \left(\frac{a,\ m}{l_t}\right),$$

das *Charakterensystem der Zahl a im Körper $k(\sqrt{m})$*.

Will man nun diese Definition auf Ideale eines Zahlkörpers erweitern, so hat man reelle und imaginäre Körper zu unterscheiden. Als eine zweckmäßige Ausdehnung der ursprünglichen Definition erweist sich die folgende Festsetzung[1]):

Ist $\mathfrak{a}$ ein Ideal eines *imaginären* Körpers $k(\sqrt{m})$, so kann $\bar{n}=n(\mathfrak{a})$ stets als positive Zahl vorausgesetzt werden, und man bezeichnet als *Charakterensystem des Ideals $\mathfrak{a}$ im Körper $k(\sqrt{m})$* die Gesamtheit der $r=t$ Einheiten ± 1:

1) Vergl. Hilbert, Zahlber. § 65, S. 291. Eine andere Definition des Charakterensystems ist in der Anmerk. S. 173 erwähnt.

$$\left(\frac{\bar{n},\,m}{l_1}\right),\quad \left(\frac{\bar{n},\,m}{l_2}\right)\ \ldots\ \left(\frac{\bar{n},\,m}{l_t}\right).$$

Ist dagegen $\mathfrak{a}$ ein Ideal eines reellen Körpers $k(\sqrt{m})$, so stellt man zuerst das Charakterensystem E der Zahl -1 in diesem Körper auf, und unterscheidet dann zwei Fälle:

1. Das Charakterensystem E besteht aus lauter positiven Einheiten.
2. Das Charakterensystem E enthält positive und negative Einheiten.

Im ersten Fall ist $\bar{n} = n(\mathfrak{a})$ positiv, und man bezeichnet die Gesamtheit der $r(=t)$ Einheiten, welche das Charakterensystem der Zahl $\bar{n}$ bilden, als das *Charakterensystem des Ideals* $\mathfrak{a}$.

Im zweiten Fall sei etwa l_t eine Primzahl, für welche

$$\left(\frac{-1,\,m}{l_t}\right) = -1$$

ist; dann wählt man in $\bar{n} = \pm n(\mathfrak{a})$ dasjenige Vorzeichen $+$ oder $-$, für das

$$\left(\frac{\bar{n},\,m}{l_t}\right) = +1$$

wird, setzt $r = t - 1$ und bezeichnet als Charakterensystem des Ideals $\mathfrak{a}$ im Körper $k(\sqrt{m})$ die r Einheiten:

$$\left(\frac{\bar{n},\,m}{l_1}\right),\quad \left(\frac{\bar{n},\,m}{l_2}\right)\ \ldots\ \left(\frac{\bar{n},\,m}{l_r}\right).$$

Das Charakterensystem eines *Hauptideals* besteht nach der allgemeinen Definition offenbar aus lauter *positiven* Einheiten.

Beispiele. 1. *Imaginärer Körper* $k(\sqrt{-21})$, $d = -84$.

Für die Aufstellung eines Charakterensystems kommen in Betracht die Primzahlen $l_1 = 2$, $l_2 = 3$, $l_3 = 7$. Z. B. ergibt sich für die Zahl -1:

$$\left(\frac{-1,\,-21}{2}\right) = (-1)^{-1\cdot -11} = -1,\quad \left(\frac{-1,\,-21}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$
$$\left(\frac{-1,\,-21}{7}\right) = \left(\frac{-1,\,-21}{7}\right) = +1;$$

ferner für die Zahl 3:

$$\left(\frac{3,\,-21}{2}\right) = -1,\quad \left(\frac{3,\,-21}{3}\right) = \left(\frac{7}{3}\right) = +1,\quad \left(\frac{3,\,-21}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

Für das ambige Primideal $(2,\ 1+\sqrt{-21})$ ist $\bar{n} = 2$, und man erhält als Charakterensystem:

$$\left(\frac{2,\,-21}{2}\right) = -1,\quad \left(\frac{2,\,-21}{3}\right) = \left(\frac{2}{3}\right) = -1,\quad \left(\frac{2,\,-21}{7}\right) = +1.$$

Schließlich sei noch $\mathfrak{a} = (5,\ 3+\sqrt{-21})$ $\bar{n} = 5$, dann ergibt sich:

$$\left(\frac{5,\,-21}{2}\right)=1,\quad \left(\frac{5,\,-21}{3}\right)=\left(\frac{5}{3}\right)=-1,\quad \left(\frac{5,\,-21}{7}\right)=\left(\frac{5}{7}\right)=-1.$$

Für irgend ein Hauptideal (α) ist das Charakterensystem offenbar $+1,\ +1,\ +1$.

2. Beispiel. *Reeller Körper* $k(\sqrt{34})$, $d=136$ und $l_1=2$, $l_2=17$. Zunächst braucht man das Charakterensystem von -1; es wird:

$$\left(\frac{-1,\,34}{2}\right)=(-1)^{\frac{1-1}{8}+\frac{1-1}{2}\cdot\frac{17-1}{2}}=+1,$$

$$\left(\frac{-1,\,34}{17}\right)=\left(\frac{-1}{17}\right)=+1,$$

man hat also $r=t=2$ zu nehmen.

Für ein Hauptideal ergibt sich als Charakterensystem stets: $+1,\ +1$.

Für $\mathfrak{a}=(3,\ 1+\sqrt{34})$ ist $\bar{n}=+3$ zu nehmen, dann wird das Charakterensystem von $\mathfrak{a}$:

$$\left(\frac{3,\,34}{2}\right)=(-1)^{1+8}=-1,\quad \left(\frac{3,\,34}{17}\right)=\left(\frac{3}{17}\right)=-1.$$

3. Beispiel. *Reeller Körper* $k(\sqrt{51})$, $d=204$, $l_1=2$, $l_3=3$, $l_2=17$. Das Charakterensystem der Zahl -1 ist:

$$\left(\frac{-1,\,51}{2}\right)=-1,\quad \left(\frac{-1,\,51}{3}\right)=\left(\frac{-1}{3}\right)=-1,\quad \left(\frac{-1,\,51}{17}\right)=\left(\frac{-1}{17}\right)=1.$$

Wir setzen daher jetzt $l_3=3$, $r=2$, und bekommen als Charakterensystem eines Hauptideals $+1,\ +1$.

Sei nun ferner $\mathfrak{a}=(5,\ 6+\sqrt{51})$, so wird

$$\left(\frac{\bar{n},\,51}{3}\right)=\left(\frac{\bar{n}}{3}\right)=\left(\frac{\pm 5}{3}\right)=+1,$$

wenn $\bar{n}=-5$ genommen wird. Man erhält dann für das Ideal $\mathfrak{a}$ als Charakterensystem:

$$\left(\frac{-5,\,51}{2}\right)=-1,\quad \left(\frac{-5,\,51}{17}\right)=\left(\frac{5}{17}\right)=-1.$$

Eine unmittelbare Folgerung aus der Definition des Normenrestsymbols und des Charakterensystems eines Ideals ist nun der folgende Satz.

Satz. *Alle Ideale einer und derselben Idealklasse haben dasselbe Charakterensystem.*

Beweis. $\mathfrak{a}$ und $\mathfrak{b}$ seien zwei Ideale des Körpers $k(\sqrt{m})$, welche derselben Idealklasse angehören. Dann gibt es also zwei ganze Zahlen α, β des Körpers, so daß die Beziehung gilt:

$$(\alpha)\mathfrak{a}=(\beta)\mathfrak{b}. \tag{1}$$

Bezeichnet $n(\alpha)$ bezw. $n(\beta)$ die Norm der Zahl α resp. der Zahl β und setzt man der Definition für das Charakterensystem eines Ideals $\mathfrak{a}$ entsprechend:

$$N = \pm\, n(\alpha\mathfrak{a}), \quad N_1 = \pm\, n(\beta\mathfrak{b}),$$

also

$$N = N_1$$

und

$$\bar{n} = \pm\, n(\mathfrak{a}), \quad \bar{n}_1 = \pm\, n(\mathfrak{b}),$$

so gilt für alle Primzahlen p, insbesondere für $p = l_1, l_2 \ldots l_r$:

$$\left(\frac{N,\, m}{p}\right) = \left(\frac{n(\alpha),\, m}{p}\right)\left(\frac{\bar{n},\, m}{p}\right) = \left(\frac{\bar{n},\, m}{p}\right)$$

und

$$\left(\frac{N_1,\, m}{p}\right) = \left(\frac{n(\beta),\, m}{p}\right)\left(\frac{\bar{n}_1,\, m}{p}\right) = \left(\frac{\bar{n}_1,\, m}{p}\right),$$

sonach mit Rücksicht auf die Gleichung (1) oder $N = N_1$:

$$\left(\frac{\bar{n},\, m}{p}\right) = \left(\frac{\bar{n}_1,\, m}{p}\right)$$

für $p = l_1, \ldots l_r$. Der Satz ist also richtig.

29. Einteilung der Idealklassen in Geschlechter.

Es liegt nahe, nach diesem Satz alle diejenigen Klassen, welche dasselbe Charakterensystem besitzen, zu einer Gruppe zu vereinigen; man sagt alsdann, diese Klassen gehören einem **Geschlecht** an. Dasjenige Geschlecht, welches die Hauptklasse enthält, möge insbesondere das **Hauptgeschlecht** heißen. Sein Charakterensystem besteht aus lauter positiven Einheiten. In bezug auf die Zahl der Idealklassen, welche einem Geschlecht angehören, kann man nun folgenden Satz beweisen:

Satz. *Die Geschlechter, auf welche sich die Idealklassen des Körpers $k(\sqrt{m})$ verteilen, enthalten alle die gleiche Anzahl Idealklassen.*

Beweis. $H_1, H_2 \ldots H_f$ seien die Klassen aus dem Hauptgeschlecht des Körpers. Ist damit die Anzahl der Idealklassen noch nicht erschöpft, so sei K eine Klasse, welche diesem Geschlecht nicht angehört. Dann sind 1.) die Klassen $KH_1, KH_2 \ldots KH_f$ voneinander verschieden, und sie haben 2.) alle ein und dasselbe Charakterensystem, oder sie gehören *einem* Geschlechte an. In der Tat, wenn $\mathfrak{j}, \mathfrak{h}_1 \ldots \mathfrak{h}_f$ Ideale aus den resp. Klassen $K, H_1 \ldots H_f$ sind, so ist

1. $\mathfrak{j}\mathfrak{h}_1$ nicht äquivalent $\mathfrak{j}\mathfrak{h}_2$,

weil sonst $\mathfrak{h}_1 \sim \mathfrak{h}_2$ sein müßte, also ist auch $KH_1 \neq KH_2$.

2. Für die Normenrestsymbole gilt zu allen Werten $l_1, \ldots l_r$:

$$\left(\frac{\pm n\,\mathfrak{j}\mathfrak{h}_1,\, m}{l_i}\right) = \left(\frac{\pm n\,\mathfrak{j}\cdot n\,\mathfrak{h}_1,\, m}{l_i}\right)$$

$$= \left(\frac{\pm n\,\mathfrak{j},\, m}{l_i}\right)\left(\frac{\pm n\,\mathfrak{h}_1,\, m}{l_i}\right),$$

usw. für $\mathfrak{h}_2, \mathfrak{h}_3 \ldots \mathfrak{h}_f$. Es haben daher alle Klassen $KH_1, KH_2 \ldots KH_f$ dasselbe Charakterensystem. Ist nun mit den Klassen $H_1, H_2 \ldots H_f$, $KH_1 \ldots KH_f$ die Gesamtheit der Idealklassen erschöpft, so ist der Satz bewiesen. Im anderen Fall sei L eine Klasse, welche nicht unter den aufgeführten Klassen schon enthalten ist, dann kann zunächst das Charakterensystem der Klasse L nicht mit dem des Hauptgeschlechts, sodann aber auch nicht mit dem Charakterensystem der Klassen $KH_1, \ldots KH_f$ übereinstimmen.

L kann nicht dem Hauptgeschlecht angehören, da ja die Klassen desselben zuerst in vollständiger Weise ausgesucht waren.

Es sei nun $\mathfrak{l}$ ein Ideal der Klasse L und $\mathfrak{j}$ ein Ideal der Klasse K (bezw. KH_1, wenn H_1 die Hauptklasse ist), und es bezeichne (ι) ein Hauptideal, welches durch $\mathfrak{j}^1$ teilbar ist; dann existiert ein Ideal $\mathfrak{a}$ des Körpers derart, daß

$$(\iota)\mathfrak{l} = \mathfrak{j}\cdot\mathfrak{a}$$

wird, und es ist also:

$$\left(\frac{\pm n(\iota\mathfrak{l}),\, m}{l_i}\right) = \left(\frac{\pm n(\mathfrak{l}),\, m}{l_i}\right)$$

$$\left(\frac{\pm n(\mathfrak{l}),\, m}{l_i}\right) = \left(\frac{\pm n(\mathfrak{j}),\, m}{l_i}\right)\left(\frac{\pm n(\mathfrak{a}),\, m}{l_i}\right)$$

$$(\text{für } i = 1, 2, \ldots r).$$

Angenommen nun, es besäße L dasselbe Charakterensystem wie K, resp. KH_s, so müßte

$$\left(\frac{\pm n(\mathfrak{a}),\, m}{l_i}\right) = +1$$

sein für $i = 1, \ldots r$. Dann würde $\mathfrak{a}$ einer der Klassen des Hauptgeschlechtes anhören, oder es wäre:

$$L = KH_s.$$

L müßte also entgegen der Voraussetzung unter den angeführten Klassen schon enthalten sein.

Die Klassen $KH_1, \ldots KH_f$ und *nur diese* gehören wieder einem Geschlecht an. Dasselbe läßt sich in genau analoger Weise von den neuen Klassen

$$LH_1, \ldots LH_f$$

zeigen, und es ist klar, daß durch die Fortsetzung des angefangenen Prozesses die Idealklassen sämtlich erschöpft werden, womit der Satz bewiesen ist.

Aus diesem Satz kann schon eine sehr wichtige Folgerung gezogen werden:

Enthält die Diskriminante eines Körpers $k(\sqrt{m})$ nur eine einzige Primzahl, so ist die Anzahl der Idealklassen ungerade, und das Charakterensystem einer Klasse besteht nur aus der einzigen Zahl $+1$ oder -1. Danach wären nun überhaupt nur zwei Geschlechter möglich, weil aber die Klassenanzahl ungerade ist, so müssen die sämtlichen Klassen einem einzigen Geschlecht angehören, dessen Charakterensystem $+1$ *oder* -1 ist. Idealklassen, die das Charakterensystem -1 resp. $+1$ besitzen, gibt es nicht.

Dieser Fall ist ein Beispiel für einen viel allgemeineren Satz, zu dessen Ableitung der folgende Satz die Grundlage bildet:

Satz. *Sind n und m zwei quadratfreie ganze rationale Zahlen, die nicht beide negativ sind, so ist*

$$\prod_p \left(\frac{n,\, m}{p}\right) = +1,$$

wenn das Produkt auf der linken Seite über sämtliche positive rationale Primzahlen p erstreckt wird.

Beweis. Zunächst ist für jede ungerade Primzahl p, welche weder in n noch in m aufgeht,

$$\left(\frac{n,\, m}{p}\right) = +1.$$

Wenn n und m *positive* ungerade und teilerfremde Zahlen sind, so bleiben danach bei der Berechnung des Wertes von:

$$\prod_p \left(\frac{n,\, m}{p}\right)$$

außer $p = 2$ nur diejenigen Primzahlen p zu berücksichtigen, welche in n oder m aufgehen; nach Entwicklung des Produktes $\prod\limits_p$ behält man einfach:

$$\prod_p \left(\frac{n,\, m}{p}\right) = \left(\frac{n,\, m}{2}\right)\cdot\left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_\mu}\right)\cdot\left(\frac{m}{q_1}\right)\cdots\left(\frac{m}{q_\nu}\right)$$

übrig, wo $p_1, p_2, \ldots$ resp. $q_1, q_2 \ldots$ die voneinander verschiedenen Primzahlen sind, welche in n resp. in m aufgehen.

Nach dem allgemeinen Jacobischen quadratischen Reziprozitätsgesetz (vergl. S. 122) ist aber:

$$\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right)=\left(\frac{n}{p_1}\right)\cdot\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_\mu}\right)\cdot\left(\frac{m}{q_1}\right)\cdots\left(\frac{m}{q_\nu}\right)=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}},$$

da andererseits auch

$$\left(\frac{n,\,m}{2}\right)=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$$

ist, so erhält man schließlich als Resultat dieses einfachsten Falles:

$$\prod_p\left(\frac{n,\,m}{p}\right)=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}\cdot(-1)^{\frac{n-1}{2}\,\frac{m-1}{2}}=+1.$$

Sind jetzt ferner m und n wieder ungerade teilerfremde Zahlen und ist m positiv, dagegen n eine negative Zahl etwa gleich $-n_1$, so daß also n_1 positiv ist, so ergibt sich:

$$\prod_p\left(\frac{n,\,m}{p}\right)=\prod\left(\frac{-n_1,\,m}{p}\right)=\prod\left(\frac{-1,\,m}{p}\right)\cdot\prod\left(\frac{n_1,\,m}{p}\right);$$

hierin ist der letzte Faktor wieder $+1$, während für den ersten Faktor nach den allgemeinen Sätzen über das Hilbertsche Symbol, und unter Berücksichtigung des Jacobischen Reziprozitätsgesetzes die Gleichung gilt:

$$\prod_p\left(\frac{-1,\,m}{p}\right)=\left(\frac{-1,\,m}{2}\right)\left(\frac{-1}{m}\right).$$

Es ist aber:

$$\left(\frac{-1,\,m}{2}\right)=(-1)^{\frac{m-1}{2}},\quad\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}},$$

also wird auch hier wiederum:

$$\prod\left(\frac{n,\,m}{p}\right)=+1.$$

Falls andererseits m negativ gleich $-m_1$, dagegen n positiv ist, gelten nach dem Vertauschungssatz für das Hilbertsche Symbol die Gleichungen:

$$\prod_p\left(\frac{n,\,-m_1}{p}\right)=\prod_p\left(\frac{-m_1,\,n}{p}\right)=+1.$$

Sind ferner n, m ungerade Zahlen, die nur einen gemeinsamen Primfaktor r enthalten, und setzt man $m=r\cdot m_1$, $n=rn_1$, so wird:

$$\prod_p\left(\frac{n,\,m}{p}\right)=\left(\frac{n,\,m}{2}\right)\left(\frac{-m_1n_1}{r}\right)\left(\frac{n}{m_1}\right)\left(\frac{m}{n_1}\right)=+1.$$

Genau ebenso erledigt sich der weitere Fall, daß die ungeraden Zahlen n, m nicht einen, sondern mehrere Primfaktoren r, s ... ge-

mein haben. Es bleiben daher nur noch die Fälle zu betrachten, in denen eine oder beide Zahlen m und n den Faktor 2 enthalten.

Es sei erstens m ungerade und n gerade, etwa $n = 2n_1$, dann gelten folgende Gleichungen:

$$\prod_p \left(\frac{2n_1, m}{p}\right) = \prod_p \left(\frac{2, m}{p}\right) \cdot \prod_p \left(\frac{n_1, m}{p}\right) = \prod_p \left(\frac{2, m}{p}\right);$$

da aber alsdann unter Benutzung des Jacobischen Symbols:

$$\prod_p \left(\frac{2, m}{p}\right) = \left(\frac{2, m}{2}\right) \cdot \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} \cdot (-1)^{\frac{m^2-1}{8}} = +1$$

wird, so ist auch jetzt wieder:

$$\prod_p \left(\frac{2n_1, m}{p}\right) = +1.$$

Ist zweitens n ungerade und m gerade, $m = 2m_1$, so folgt durch Zuhilfenahme der für alle Fälle geltenden Umkehrungsformel:

$$\left(\frac{n, m}{p}\right) = \left(\frac{m, n}{p}\right)$$

wiederum:

$$\prod_p \left(\frac{n, 2m_1}{p}\right) = 1.$$

Wenn schließlich n und m gerade sind, etwa $n = 2n_1$, $m = 2m_1$, so ist:

$$\prod_p \left(\frac{2n_1, 2m_1}{p}\right) = \prod_p \left(\frac{2, 2m_1}{p}\right) \prod_p \left(\frac{n_1, 2m_1}{p}\right) = \prod_p \left(\frac{2, 2m_1}{p}\right)$$

$$\prod_p \left(\frac{2, 2m_1}{p}\right) = \prod_p \left(\frac{2, 2}{p}\right) \prod_p \left(\frac{2, m_1}{p}\right) = \prod_p \left(\frac{2, 2}{p}\right).$$

In dem übrig bleibenden Produkt bleibt aber allein noch das Verhalten der Zahl $p = 2$ zu untersuchen, da ohnehin für alle anderen ungeraden Primzahlen p:

$$\left(\frac{2, 2}{p}\right) = +1$$

ist. Nun ist aber im Körper $k(\sqrt{2})$ die Zahl 2 die Norm der ganzen Zahl $2 + \sqrt{2}$, d. h.:

$$\left(\frac{2, 2}{2}\right) = +1,$$

also ist auch für den letzten Fall:

$$\prod_p \left(\frac{2n_1,\ 2m_1}{p}\right) = +1,$$

und es ist somit der Satz in allen Teilen bewiesen.

Zur Gültigkeit des Satzes ist wirklich notwendig, daß wenigstens eine der beiden Zahlen n, m, positiv ist. Sind n *und* m negative Zahlen, etwa $n = -n_1$, $m = -m_1$, so daß n_1, m_1 positiv sind, dann dürfen wir nach den bisherigen Ergebnissen schreiben:

$$\prod_p \left(\frac{-n_1,\ -m_1}{p}\right) = \prod_p \left(\frac{-1,\ -m_1}{p}\right) \prod_p \left(\frac{n_1,\ -m_1}{p}\right)$$
$$= \prod \left(\frac{-1,\ -1}{p}\right) \prod \left(\frac{-1,\ m_1}{p}\right) = \left(\frac{-1,\ -1}{2}\right).$$

Weil aber:

$$\left(\frac{-1,\ -1}{2}\right) = -1$$

ist, so gilt also für zwei negative Zahlen n, m die Gleichung:

$$\prod_p \left(\frac{n,\ m}{p}\right) = -1.$$

Aus dem vorstehenden Satz folgt nun eine Bemerkung, welche für die Untersuchung über die Geschlechter ganz fundamental ist.

Ist nämlich $n(\mathrm{j})$ die Norm eines Ideals in dem Körper $k(\sqrt{m})$, so ist laut Definition für die Berechnung des Charakterensystems des Ideals j: $\bar{n} = n(\mathrm{j})$ stets positiv zu nehmen für ein negatives m, also ist für $\bar{n}$ und m die Bedingung des vorhergehenden Satzes erfüllt, daß wenigstens eine der beiden Zahlen $\bar{n}$, m positiv ist.

Ist m positiv, so kann zwar $\bar{n} = \pm n(\mathrm{j})$ negativ oder positiv werden, aber es gilt doch wieder die Voraussetzung des vorhin bewiesenen Satzes, d. h. es ist stets:

$$\prod_p \left(\frac{\bar{n},\ m}{p}\right) = +1.$$

Es sei nun $\bar{n} = \pm n(\mathrm{j})$ die Norm eines Nichthauptideals, das, unbeschadet der Allgemeinheit, als frei von rationalen Faktoren vorausgesetzt werden darf. Dann kann man setzen:

$$1 = \prod_p \left(\frac{\bar{n},\ m}{p}\right) = \prod_p{}' \left(\frac{\bar{n},\ m}{p}\right),$$

wo nunmehr das mit Π' bezeichnete Produkt rechts bloß über die Primfaktoren von $\bar{n}$ resp. m und außerdem etwa noch $p = 2$ (falls m und $\bar{n}$ ungerade sind) zu erstrecken ist.

Bezeichnen $q_1, q_2, \ldots q_\nu$ die ungeraden Primfaktoren von $\bar{n}$,

welche nicht zugleich in m aufgehen, so ist nach der Voraussetzung über $\bar{n}$, wonach es die Norm eines Nichthauptideals ist:

$$\left(\frac{m}{q_1}\right) = +1, \quad \left(\frac{m}{q_2}\right) = +1, \ldots \quad \left(\frac{m}{q_\nu}\right) = +1,$$

und es bleibt daher die Gleichung übrig:

$$\overline{\prod_p} \left(\frac{\bar{n}, m}{p}\right) = +1,$$

indem jetzt das Produkt $\overline{\Pi}$ nur noch genommen ist über alle Primfaktoren p von m und ev. außerdem $p = 2$.

Wenn $\prod_p{}'' \left(\frac{\bar{n}, m}{p}\right)$ das Produkt bezeichnet, welches erstreckt ist über alle und nur über die Primfaktoren p der Diskriminante des Körpers $k(\sqrt{m})$, so ist nun bewiesen, daß:

$$\prod_p{}'' \left(\frac{\bar{n}, m}{p}\right) = +1$$

wird, wenn $m \equiv 3$, (4) oder $m \equiv 2$, (4) ist.

Ist andererseits $m \equiv 1$, (4), so ist nach derselben Bezeichnung:

$$1 = \overline{\prod_p} \left(\frac{\bar{n}, m}{p}\right) = \left(\frac{\bar{n}, m}{2}\right) \prod_p{}'' \left(\frac{\bar{n}, m}{p}\right).$$

Die Zahl $\bar{n}$ (als Norm eines Ideals) enthält den einfachen Faktor 2 nur, wenn 2 in $k(\sqrt{m})$ zerfällt, d. h. wenn also $m \equiv 1$, (8) ist. Mit Benützung der Formeln für $\left(\frac{\bar{n}, m}{2}\right)$ auf S. 133 und 135 erhält man darum für gerades und ungerades $\bar{n}$

$$\prod_p{}'' \left(\frac{\bar{n}, m}{p}\right) = +1.$$

Berücksichtigt man noch, daß das Charakterensystem für alle Hauptideale aus lauter positiven Einheiten besteht, und beachtet man ferner, daß das Produkt Π'' als Faktoren die sämtlichen Größen $\left(\frac{\bar{n}, m}{p}\right)$ enthält, welche das Charakterensystem des Ideals $\mathfrak{j}$ bilden, so kann man das Resultat der bisherigen Betrachtungen so formulieren:

Satz. *Das Produkt aller r Einheiten des Charakterensystems eines beliebigen Ideals ist stets gleich* $+1$. Oder: *Ein System von r Einheiten* ± 1 *kann nur dann das Charakterensystem eines Körperideals darstellen, wenn das Produkt der r Einheiten gleich* $+1$ *ist.*

Die Anzahl der denkbaren Charakterensysteme ist 2^r, nämlich ebenso groß wie die Anzahl der voneinander verschiedenen Anord-

nungen der Einheiten $+1$ und -1 auf r Stellen. Die Anzahl dieser Anordnungen für irgend eine Zahl n bestimmt man durch den Schluß von e auf $e+1$: Für $e=1$ gibt es zwei Anordnungen $\begin{cases} +1 \\ -1 \end{cases}$. Wenn es für e Einheiten N voneinander verschiedene Anordnungen gibt, so erhält man die sämtlichen Anordnungen für $e+1$ Einheiten offenbar, indem man jeder der N Reihen zuerst $+1$ und dann -1 beifügt, wodurch also für $e+1$ Einheiten $2 \cdot N$ Anordnungen sich ergeben. Man schließt daher durch Induktion, daß $N = 2^n$ wird für die Anordnungen der Einheiten ± 1 zu n Stellen.

Enthalten die N Anordnungen von e Einheiten N_1 resp. N_2 Reihen mit einer geraden resp. ungeraden Anzahl negativer Einheiten, so enthalten die $2N$ Anordnungen von $e+1$ Einheiten offenbar $N_2 + N_1 = N$ Reihen mit einer geraden und ebensoviele Reihen mit einer ungeraden Anzahl negativer Einheiten. Das Produkt der $e+1$ Einheiten in diesen Reihen ist also $+1$. Natürlich gilt dieses Resultat für die Zahl n oder eine beliebige Zahl r selbst, d. h. unter den sämtlichen möglichen Anordnungen der Einheiten ± 1 zu r Stellen, enthält genau die Hälfte eine ungerade Anzahl negativer Einheiten. Unter den 2^r Anordnungen von r Einheiten sind die Hälfte so beschaffen, daß das Produkt der Einheiten $+1$ ist, und diese Anordnungen sind diejenigen, denen allein *mögliche* Charakterensysteme oder *mögliche* Geschlechter entsprechen.

Man kann daher den Satz aussprechen:

In einem quadratischen Körper $k(\sqrt{m})$ gibt es höchstens 2^{r-1} Geschlechter.

Es ist sicher, daß der Hälfte der denkbaren Charakterensysteme *keine* Geschlechter entsprechen können; die Frage aber, ob nun allen bleibenden Charakterensystemen, deren Produkt $+1$ ist, auch wirklich Geschlechter entsprechen, ist damit nicht entschieden und bedarf der weiteren Untersuchung. In der Tat läßt sich beweisen, daß genau 2^{r-1} Geschlechter in dem quadratischen Körper existieren. Zu diesem Nachweis ist vor allem eine sorgfältige Untersuchung der Eigenschaften der *ambigen* Klassen des Körpers erforderlich.

30. Die ambigen Klassen.

Wenn $\mathfrak{a}$ und $\mathfrak{a}'$ zwei konjugierte Ideale eines quadratischen Zahlkörpers sind, so bestimmen dieselben *im allgemeinen* auch zwei verschiedene (reziproke) Klassen des Körpers. Diejenigen speziellen

Klassen des Körpers, wie die Hauptklasse, welche ein Nichthauptideal $\mathfrak{a}$ und sein konjugiertes Ideal $\mathfrak{a}'$ zugleich enthalten, heißen *ambige Klassen.*

Jedes Ideal $\mathfrak{j}$ einer ambigen Idealklasse ist alsdann äquivalent mit seinem konjugierten Ideal, d. h. es ist:

$$\mathfrak{j} \sim \mathfrak{j}'.$$

Das Quadrat A^2 einer ambigen Klasse A ist stets die Hauptklasse, und umgekehrt, wenn das Quadrat einer Idealklasse die Hauptklasse ist, so ist diese Klasse *ambig.*

Offenbar sind alle diejenigen Klassen ambig, welche ambige Ideale enthalten, es ist aber auch denkbar, daß es ambige Klassen gibt, welche keine ambigen Ideale enthalten.

Um die Anzahl der voneinander verschiedenen ambigen Idealklassen des Körpers zu finden, verfährt man so, daß man zunächst die Anzahl derjenigen verschiedenen Idealklassen bestimmt, welche ambige Ideale enthalten, und dazu die Anzahl der ambigen Klassen, welche selbst keine ambigen Ideale enthalten, hinzufügt.

Nach dem Satz über die Idealteiler der Körperdiskriminante ist jede Primzahl, welche in der Diskriminante aufgeht, gleich dem Quadrat eines ambigen Primideals. Bezeichnen daher $l_1, \dots l_t$ die sämtlichen voneinander verschiedenen rationalen Primfaktoren der Diskriminante und $\mathfrak{l}_1, \dots \mathfrak{l}_t$ die resp. Primidealteiler dieser Primzahlen, so hat man damit t verschiedene ambige Primideale.

Die Produkte von je zweien, je dreien usw. (verschiedenen) dieser Primideale sind wieder ambige Ideale, und da man, abgesehen von dem Produkt der sämtlichen Ideale $\mathfrak{l}_t$, welches gleich $(\sqrt{m})$ ist,

$$2^t - 1$$

derartige Produkte, die Primideale selbst mitgezählt, bilden kann, so hat man in dem quadratischen Körper $2^t - 1$ verschiedene ambige Ideale, oder 2^t, wenn das Ideal (1) dazu gerechnet wird.

Um die Anzahl der verschiedenen ambigen Klassen, welche diese ambigen Ideale bestimmen, zu erhalten, hat Herr Hilbert zunächst den Begriff der *unabhängigen* ambigen Klassen eingeführt:

Definition. Ein System ambiger Klassen heißt ein System voneinander *unabhängiger* ambiger Klassen, wenn keine Klasse sich durch das Produkt irgend welcher Potenzen der anderen Klassen des Systems ausdrücken läßt und wenn keine unter ihnen die Hauptklasse ist.

Für die ambigen unabhängigen Klassen, welche aus den ambigen

Primidealen des Körpers hervorgehen, gilt jetzt der folgende fundamentale Satz:

Satz. *Die t ambigen Primideale, welche in der Diskriminante eines quadratischen Körpers $k(\sqrt{m})$ aufgehen, bestimmen 1.) im Falle eines imaginären Körpers stets $t-1$ unabhängige ambige Klassen, 2.) im Falle eines reellen Körpers $t-2$ oder $t-1$ unabhängige ambige Klassen, je nachdem die Norm der Grundeinheit des Körpers $+1$ oder -1 ist. Den beiden Fällen entsprechend gibt es in diesen Körpern entweder 2^{t-1} oder 2^{t-2} resp. 2^{t-1} verschiedene ambige Klassen mit ambigen Idealen.*

Beweis. 1.) Zunächst möge $k(\sqrt{m})$ einen *imaginären* Körper bedeuten.

Für $k(\sqrt{-1})$ ist:

$$d = -4, \quad l_1 = 2, \quad t = 1,$$

das einzige ambige Ideal des Körpers ist:

$$\mathfrak{l}_1 = (1 + \sqrt{-1}) \sim 1,$$

es existiert also eine ambige Klasse: die Hauptklasse.

Für $k(\sqrt{-2})$ ist

$$d = -8, \quad l_1 = 2, \quad t = 1,$$

und da

$$\mathfrak{l}_1 = (\sqrt{-2}) \sim 1$$

ist, so ist also wieder keine unabhängige ambige Klasse vorhanden. Das gleiche ergibt sich für $k(\sqrt{-3})$.

Die beiden Körper $k(\sqrt{-1})$ und $k(\sqrt{-3})$ sind die einzigen imaginären Körper, in denen Einheiten existieren, die von ± 1 verschieden sind. Für jeden anderen imaginären Körper $k(\sqrt{m})$, für den $|m| > 3$ ist, sind ± 1 die einzigen Einheiten.

Es sei $(\alpha) = (x + y\omega)$ ein ambiges Hauptideal des imaginären Körpers $k(\sqrt{m})$, so muß

$$x + y\omega = \varepsilon \cdot (x + y\omega')$$

sein, wo ε eine Einheit des Körpers bedeutet. Ist nun $|m| > 3$, dann müßte entweder

$$x + y\omega = \quad x + y\omega' \tag{1}$$

oder

$$x + y\omega = -x - y\omega' \tag{2}$$

sein.

Die Gleichung (1) ist überhaupt nur möglich, wenn $y = 0$ und x gleich einer beliebigen ganzen rationalen Zahl a gesetzt wird.

Die Gleichung (2) dagegen liefert

1. für $\omega = \sqrt{m}$: $\quad x = 0, \quad y = b, \quad$ spez. $\quad y = 1,$

2. für $\omega = \frac{1+\sqrt{m}}{2}$: $\quad x = -b, \quad y = 2b,$

woraus folgt, daß

$$(1), \quad (\sqrt{m})$$

die einzigen ambigen Hauptideale des Körpers sind.

Ist nun $m \equiv 1, (4)$, oder $m \equiv 2, (4)$, so wird das Produkt aller im Körper vorhandenen ambigen Ideale ein Hauptideal:

$$\mathfrak{l}_1 \mathfrak{l}_2 \ldots \mathfrak{l}_t = (\sqrt{m});$$

falls aber $m \equiv 3, (4)$ ist und $\mathfrak{l}_1$ das in (2) aufgehende ambige Primideal bezeichnet, wird:

$$\mathfrak{l}_2 \mathfrak{l}_3 \ldots \mathfrak{l}_t = (\sqrt{m}).$$

In beiden Fällen läßt sich also eines von allen den in $(\sqrt{m})$ aufgehenden Idealen, etwa $\mathfrak{l}_t$, durch $(\sqrt{m})$ und die übrigen Ideale ausdrücken, so daß man jedesmal höchstens $t-1$ unabhängige ambige Klassen bekommen kann.

Es kann aber auch niemals eine Äquivalenz gelten von der Art:

$$\mathfrak{l}_1 \sim \mathfrak{l}_2 \mathfrak{l}_3 \ldots \mathfrak{l}_\nu,$$

wenn $m \equiv 1$ bezw. $m \equiv 2, (4)$ ist, oder von der Art:

$$\mathfrak{l}_2 \sim \mathfrak{l}_3 \ldots \mathfrak{l}_\nu,$$

wenn $m \equiv 3, (4)$ ist, für $\nu \leqq t-1$, denn es müßte alsdann

$$\mathfrak{l}_1 \mathfrak{l}_2 \ldots \mathfrak{l}_\nu \sim 1,$$

resp.

$$\mathfrak{l}_2 \mathfrak{l}_3 \ldots \mathfrak{l}_\nu \sim 1$$

sein, was nach der zuerst gemachten Bemerkung über die im Körper vorhandenen ambigen Hauptideale nicht möglich ist. Daher erzeugen die $t-1$ Ideale $\mathfrak{l}_1, \mathfrak{l}_2, \ldots \mathfrak{l}_{t-1}$ ebensoviele unabhängige ambige Klassen.

Bildet man jetzt ferner die Produkte der $t-1$ Primideale $\mathfrak{l}_1, \mathfrak{l}_2, \ldots \mathfrak{l}_{t-1}$ zu je zweien, je dreien usw. usw., so entsteht ein System von $2^{t-1}-1$ ambigen Idealen, in dem keine zwei Ideale äquivalent sind und kein Ideal Hauptideal ist; also existieren im Körper $k(\sqrt{m})$ einschließlich der Hauptklasse 2^{t-1} voneinander verschiedene Klassen, welche ambige Ideale enthalten.

2.) Nun bezeichne $k(\sqrt{m})$ einen *reellen* Körper. Die *reellen* quadratischen Körper zeigen ein verschiedenes Verhalten, je nachdem

die Norm der Grundeinheit ε gleich $+1$ oder gleich -1 ist. Im ersten Fall, wenn $n(\varepsilon) = +1$ ist, existiert im Körper $k(\sqrt{m})$ stets eine ganze Zahl, verschieden von 1 und von $\pm\sqrt{m}$, von der Beschaffenheit, daß man:

$$\varepsilon = \frac{\alpha}{\alpha'}$$

setzen kann. Aus der Gleichung $\varepsilon = \frac{\alpha}{\alpha'}$ folgt aber die Idealgleichung:

$$(\alpha) = (\alpha'),$$

und darnach stellt (α) ein ambiges Hauptideal vor, das verschieden ist von (1) und $(\sqrt{m})$. Außer (1), $(\sqrt{m})$, (α) und dem, von etwaigen rationalen Faktoren befreiten, Hauptideal $(\sqrt{m}\alpha)$ gibt es aber im Körper $k(\sqrt{m})$ kein ambiges Hauptideal, das von jenen Idealen unabhängig wäre.

Bedeutet nämlich (β) ein beliebiges ambiges Hauptideal des Körpers, so gibt es notwendig eine ganze Zahl f derart, daß $\beta = \pm\,\varepsilon^f \beta'$ wird. Da aber andererseits $\alpha^f = \varepsilon^f \alpha'^f$ ist, so wird der Quotient:

$$1.)\quad \gamma = \frac{\beta}{\alpha^f}, \qquad \text{falls } \beta = +\,\varepsilon^f \beta' \text{ ist},$$

$$2.)\quad \gamma = \frac{\beta}{\sqrt{m}\,\alpha^f}, \quad \text{falls } \beta = -\,\varepsilon^f \beta' \text{ ist},$$

eine Zahl, für welche $\frac{\gamma}{\gamma'} = +1$ ausfällt. Das ist jedoch bloß möglich, wenn γ eine rationale Zahl ist, es existiert somit außer (1), $(\sqrt{m})$, (α) und dem von rationalen Faktoren befreiten Ideal $(\alpha\sqrt{m})$ kein weiteres von jenen Idealen unabhängiges ambiges Hauptideal im Körper $k(\sqrt{m})$.

Ist zweitens die Norm der Grundeinheit des Körpers $n(\varepsilon) = -1$, so enthält der quadratische Körper nur (1) und $(\sqrt{m})$ als ambige Hauptideale.

Denn bedeutet (α) ein ambiges Hauptideal, das verschieden von (1) und von $(\sqrt{m})$ vorausgesetzt ist und durch $(\sqrt{m})$ nicht teilbar sein soll, so setze man:

$$\frac{\alpha}{\alpha'} = \pm\,\varepsilon^f.$$

Aus diesem Ansatz folgt $n(\pm\,\varepsilon^f) = +1$, und es muß der Exponent f gerade sein, weil nach Voraussetzung $n(\varepsilon) = -1$ ist. Wählt man nun ferner:

$$1.)\quad \beta = \frac{\alpha}{\varepsilon^{\frac{f}{2}}} \quad \begin{cases} \text{falls } \frac{f}{2} \equiv 0,\ (2) \text{ und } \frac{\alpha}{\alpha'} = +\varepsilon^f, \\ \text{oder falls } \frac{f}{2} \equiv 1,\ (2) \text{ und } \frac{\alpha}{\alpha'} = -\varepsilon^f \text{ ist,} \end{cases}$$

$$2.)\quad \beta = \frac{\alpha}{\sqrt{m}\,\varepsilon^{\frac{f}{2}}} \quad \begin{cases} \text{falls } \frac{f}{2} \equiv 0,\ (2) \text{ und } \frac{\alpha}{\alpha'} = -\varepsilon^f, \\ \text{oder falls } \frac{f}{2} \equiv 1,\ (2) \text{ und } \frac{\alpha}{\alpha'} = +\varepsilon^f \text{ ist,} \end{cases}$$

so ist β eine ganze Zahl, für welche jedesmal $\frac{\beta}{\beta'} = 1$ wird, also ist β eine rationale Zahl, und daher sind:

$$(\alpha) = (1) \quad \text{und} \quad (\alpha) = (\sqrt{m}),$$

die einzigen ambigen Hauptideale.

Nachdem so die in einem reellen Körper vorhandenen ambigen Hauptideale bekannt sind, erhält man das System der nichtäquivalenten ambigen Ideale und die voneinander unabhängigen ambigen Klassen auf dieselbe Weise wie vorhin im Falle eines imaginären Körpers.

Für einen reellen Körper, dessen Grundeinheit ε die Norm $n(\varepsilon) = -1$ hat, läßt sich von den t Primidealen $\mathfrak{l}_1, \ldots \mathfrak{l}_t$ eines durch $(\sqrt{m})$ und die übrigen in $(\sqrt{m})$ aufgehenden ausdrücken. Wenn aber $n(\varepsilon) = +1$ ist, lassen sich von den in $(\sqrt{m})$ resp. in (α) aufgehenden ambigen Primidealen zwei durch die übrigen und $(\sqrt{m})$ resp. (α) ausdrücken, so daß man nur noch ein System von $t-2$ inäquivalenten ambigen Nichthauptidealen übrig behält.

Man erhält also $t-1$ bezw. $t-2$ unabhängige ambige Klassen und insgesamt analog wie für imaginäre Körper 2^{t-1} resp. 2^{t-2} verschiedene ambige Idealklassen mit ambigen Idealen. Q. e. d.

Um die Frage nach der Gesamtheit der verschiedenen ambigen Klassen zu erledigen, bleibt jetzt noch zu entscheiden, in welchen Körpern ambige Klassen ohne ambige Ideale existieren, und es ist dann die Anzahl dieser Klassen zu bestimmen.

Man kommt dem Ziel einen Schritt näher, wenn man die Verhältnisse genauer betrachtet, die bei einer ambigen Klasse mit ambigen Idealen vorliegen.

Ist $\mathfrak{j}$ ein nichtambiges Ideal aus einer ambigen Klasse des quadratischen Körpers $k(\sqrt{m})$ und γ eine solche Zahl desselben, daß:

$$(\gamma)\mathfrak{j} = \mathfrak{j}',$$

ferner:

$$n(\gamma) = +1$$

wird, so enthält die Klasse sicher ein ambiges Ideal. Denn weil $n(\gamma) = +1$

ist, kann man eine ganze Zahl β des Körpers k angeben von der Beschaffenheit, daß:

$$\gamma = \frac{\beta}{\beta'},$$

also weiter:

$$(\beta)\mathfrak{j} = (\beta')\mathfrak{j}'$$

wird. Es ist daher $(\beta)\mathfrak{j}$ entweder selbst ein ambiges Ideal, oder doch das Produkt eines ambigen Ideals mit rationalen Faktoren.

Eine ambige Klasse ohne ambiges Ideal kann daher nur existieren, wenn $(\gamma)\mathfrak{j} = \mathfrak{j}'$ und $n(\gamma) = -1$ ist. Das letztere ist aber überhaupt bloß für einen reellen Körper möglich. Wäre nun für einen solchen reellen Körper zwar $n(\gamma) = -1$, die Norm der Grundeinheit ε indessen gleich -1, so hätte man:

$$n(\varepsilon\gamma) = +1,$$

und man könnte:

$$\varepsilon\gamma = \frac{\beta}{\beta'}$$

setzen, so daß man wieder $(\beta)\mathfrak{j} = (\beta')\mathfrak{j}'$ erhielte und die Klasse also das ambige Ideal $(\beta)\mathfrak{j}$ enthielte.

Nach diesen Erörterungen bleibt noch die Möglichkeit, die der folgende Satz ausspricht:

Satz. *In dem quadratischen Zahlkörper $k(\sqrt{m})$ existiert dann und nur dann eine ambige Klasse, welche kein ambiges Ideal enthält, wenn das Charakterensystem von -1 aus lauter positiven Einheiten besteht und wenn die Norm der Grundeinheit ε des Körpers gleich $+1$ ist.*

Die sämtlichen derartigen Klassen erhält man alsdann, indem man eine derselben mit den verschiedenen ambigen Idealklassen, welche ambige Ideale enthalten, multipliziert.

Beweis. Nach den früheren Sätzen über die Normenreste muß das Charakterensystem von -1 aus lauter positiven Einheiten bestehen, wenn -1 die Norm einer ganzen oder gebrochenen Zahl des Körpers ist. Besteht umgekehrt das Charakterensystem von -1 aus lauter positiven Einheiten, so sind alle rationalen Primteiler von m, abgesehen vom etwaigen Faktor 2, von der Form $4n + 1$, und man kann daher m stets als die Summe zweier Quadratzahlen darstellen:

$$m = u^2 + v^2.$$

Schreibt man diese Gleichung in der Form:

$$-1 = \frac{u^2 - m}{v^2}$$

so zeigt dieselbe, daß -1 die Norm einer ganzen oder gebrochenen

Zahl des reellen Körpers $k(\sqrt{m})$ ist. Diese Zahl ist notwendig *gebrochen*, da sie ja sonst eine Einheit wäre, und die Normen der Einheiten des Körpers sind nach Voraussetzung gleich $+1$.

Es möge jetzt γ eine gebrochene Zahl von der Beschaffenheit $n(\gamma) = -1$ sein, dann setze man γ gleich dem Quotienten von zwei relativ primen Idealen $\mathfrak{j}$, $\mathfrak{j}_1$, d. h.:

$$\gamma = \frac{\mathfrak{j}}{\mathfrak{j}_1} \quad \text{oder} \quad \mathfrak{j} = (\gamma) \cdot \mathfrak{j}_1.$$

Wegen $n(\gamma) = -1$ ist sodann notwendig:

$$\mathfrak{j}\mathfrak{j}' = \mathfrak{j}_1\mathfrak{j}_1'.$$

Weil aber nach Voraussetzung $\mathfrak{j}$ und $\mathfrak{j}_1$ und daher ebenso $\mathfrak{j}'$ und $\mathfrak{j}_1'$ prim zueinander sind, so folgt notwendig $\mathfrak{j}' = \mathfrak{j}_1$. Also ist $\mathfrak{j}' \sim \mathfrak{j}$, und es bestimmt $\mathfrak{j}$ eine ambige Klasse. Diese kann kein ambiges Ideal enthalten, da sonst nach unseren Betrachtungen $n(\gamma) = +1$ sein müßte, was nicht der Fall ist und was auch nicht für $\varepsilon\gamma$ zutrifft, weil $n(\varepsilon) = +1$ ist.

Unter Berücksichtigung der Betrachtungen, die dem Satz vorausgeschickt wurden, ist hiermit der erste Teil desselben bewiesen.

Bezeichnet nun $\mathfrak{j}$ ein Ideal, das selbst nicht ambig ist, jedoch eine ambige Klasse des Körpers bestimmt, und bezeichnen $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ ambige Ideale aus den verschiedenen ambigen Klassen, die im vorhergehenden Satze aufgestellt worden sind, so bestimmen die Ideale

$$\mathfrak{j}\mathfrak{a}_1, \; \mathfrak{j}\mathfrak{a}_2, \; \ldots$$

1.) lauter verschiedene und 2.) *sämtliche* ambige Klassen, die keine ambigen Ideale enthalten.

Zunächst sieht man leicht, daß keine zwei der angeschriebenen Ideale äquivalent sein können. Wäre nämlich z. B.:

$$\mathfrak{j}\mathfrak{a}_\nu \sim \mathfrak{j}\mathfrak{a}_\mu,$$

so müßte auch:

$$\mathfrak{a}_\nu \sim \mathfrak{a}_\mu$$

sein, was der Voraussetzung über die Ideale $\mathfrak{a}$ widerspricht.

Es sei ferner $\mathfrak{J}$ ein nicht ambiges Ideal aus einer der gesuchten ambigen Klassen, und es gehöre $\mathfrak{j}$ dieser Klasse nicht an. Alsdann gibt es zwei gebrochene Zahlen des Körpers γ und γ_1, für welche $n(\gamma) = n(\gamma_1) = -1$ und:

$$\frac{\mathfrak{j}}{\mathfrak{j}'} = \gamma, \quad \frac{\mathfrak{J}}{\mathfrak{J}'} = \gamma_1,$$

ist, so daß nun $\dfrac{\mathfrak{j}\mathfrak{J}}{\mathfrak{j}'\mathfrak{J}'} = \gamma\gamma_1$ wird.

Weil jetzt $n(\gamma\gamma_1) = +1$ ausfällt, kann $\gamma\gamma_1$ wieder als Quotient einer *ganzen* Zahl α und ihrer Konjugierten α' dargestellt werden. Es sei $\frac{\mathfrak{j}\mathfrak{J}}{\mathfrak{j}'\mathfrak{J}'} = \frac{\alpha'}{\alpha}$, dann ist also $(\alpha)\mathfrak{j}\mathfrak{J}$ ein ambiges Ideal, und muß notwendig gleich einem der Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ sein. Setzt man $(\alpha)\mathfrak{j}\mathfrak{J} = \mathfrak{a}$, so wird:

$$\mathfrak{J} \sim \mathfrak{j}'\mathfrak{a} \sim \mathfrak{j}\mathfrak{a}.$$

Damit ist gezeigt, daß außer den angeschriebenen Klassen keine andern ambigen Klassen der verlangten Art existieren, es ist also auch der zweite Teil des Satzes bewiesen.

[Anmerkung. Die Formulierung des ersten Teils unseres Satzes könnte auch so gewählt werden, daß man sagt, m darf außer dem ev. Faktor 2 nur Primfaktoren von der Form $4n+1$ enthalten. Die Fassung ist im engern Anschluß an die Definition des Charakterensystems eines Ideals gewählt.]

Die Zusammenfassung der eben bewiesenen Sätze ergibt den folgenden fundamentalen Satz:

Satz. *In jedem quadratischen Zahlkörper existieren 2^{r-1} verschiedene ambige Klassen.*

Beweis. 1.) Der Zahlkörper sei imaginär, dann ist $r = t$. Jede ambige Idealklasse muß notwendig auch ein ambiges Ideal enthalten, die Gesamtzahl der ambigen Klassen ist also $2^{t-1} = 2^{r-1}$.

2.) Der Zahlkörper sei reell, dann hat man drei verschiedene Unterfälle zu unterscheiden nach der Beschaffenheit des Charakterensystems von -1 und nach dem Werte der Norm der Grundeinheit.

a) Das Charakterensystem von -1 enthalte mindestens einmal die Zahl -1. In diesem Falle ist $r = t - 1$. Die Norm der Grundeinheit muß dann notwendig gleich $+1$ sein. Jede ambige Klasse des Körpers enthält auch mindestens ein ambiges Ideal, und da die Gesamtheit dieser Klassen 2^{t-2} ist, so ist überhaupt 2^{r-1} die Anzahl der verschiedenen ambigen Idealklassen.

b) Das Charakterensystem von -1 bestehe aus lauter positiven Einheiten, die Norm der Grundeinheit sei gleich -1. Dann ist $r = t$. Jede ambige Klasse enthält auch mindestens ein ambiges Ideal, und ihre Gesamtheit ist daher $2^{t-1} = 2^{r-1}$.

c) Das Charakterensystem von -1 bestehe aus lauter positiven Einheiten, die Norm der Grundeinheit sei aber gleich $+1$. Dann ist $r = t$. Der Körper enthält 2^{t-2} ambige Klassen, die je ein ambiges Ideal enthalten, und 2^{t-2} ambige Klassen ohne ambige Ideale. Die

Gesamtzahl der ambigen Klassen ist daher auch hier wieder $2 \cdot 2^{t-2} = 2^{r-1}$, wie es der Satz behauptet.

Dieses höchst merkwürdige Resultat gibt genau die Zahl, die als die Maximalzahl der möglichen Geschlechter gefunden wurde. Diese Übereinstimmung legt den Gedanken nahe, daß ein innerer Zusammenhang zwischen der Anzahl der verschiedenen ambigen Klassen und der Anzahl der Geschlechter besteht, was auch der Fall ist, wie nun gezeigt werden soll. Den Übergang zu diesem Ziel bildet ein Satz, nach dem jede Klasse des Hauptgeschlechtes als Quadrat einer Klasse des Körpers dargestellt werden kann.

31. Die Existenz der Geschlechter.

Satz. *Ist für zwei gegebene ganze rationale Zahlen n und m, die keine quadratischen Faktoren enthalten sollen und für alle Primzahlen p der Wert des Symbols $\left(\frac{n,\, m}{p}\right) = +1$, so ist n gleich der Norm einer ganzen oder gebrochenen Zahl des Körpers $k(\sqrt{m})$.*

Beweis. Wenn für *alle* Primzahlen p die Gleichung erfüllt ist:

$$\left(\frac{n,\, m}{p}\right) = +1,$$

so muß mindestens eine der beiden Zahlen n oder m positiv sein, wie früher gezeigt wurde.

Ist m negativ, so muß n positiv sein, was jedenfalls eine notwendige Voraussetzung dafür ist, daß n die Norm einer Zahl des imaginären Körpers $k(\sqrt{m})$ ist. Ist m positiv, dann kann n auch als Norm einer Zahl positiv oder negativ sein.

Wegen der Voraussetzung über n und m ist n entweder die Norm einer ganzen Zahl oder eines Ideals des Körpers, das dem Hauptgeschlecht angehört. Denn für jeden ungeraden Primteiler q von n, der nicht Divisor von m ist, gilt die Gleichung $\left(\frac{m}{q}\right) = +1$ und für jeden ungeraden Primfaktor q von n, welcher auch in m steckt $\left(\frac{m}{q}\right) = 0$, es ist also die Zahl n im Körper $k(\sqrt{m})$ zerlegbar, wenn man noch bedenkt, daß für den Fall einer geraden Zahl n, etwa $n = 2n_1$, die Zahl 2 eo ipso zerfällt, falls $m \equiv 2$, oder $m \equiv 3, (4)$ ist, und daß für $m \equiv 1, (4)$ nur dann

$$\left(\frac{2n_1,\, m}{2}\right) = (-1)^{\frac{m^2-1}{8}} = +1$$

ausfällt, wenn gleichzeitig 2 auch in $k(\sqrt{m})$ zerlegbar ist. Es möge daher $n = \pm n(\mathfrak{j})$ gesetzt werden, wo $\mathfrak{j}$ ein Ideal des Körpers bezeichnet. Da man ferner nach dem Fundamentalsatz in Nr. 16, S. 73 in der Idealklasse, welcher $\mathfrak{j}$ angehört, ein Ideal $\mathfrak{h}$ stets so wählen kann, daß dessen Norm $n(\mathfrak{h}) = n_1$ absolut genommen kleiner ist als $|\sqrt{d}|$, so gilt, unter α eine ganze oder gebrochene Zahl des Körpers verstanden, die Gleichung:

$$\mathfrak{j} = (\alpha) \cdot \mathfrak{h},$$

oder es ist:

$$n = \pm n(\mathfrak{j}) = \pm n(\alpha) \cdot n(\mathfrak{h}) = n(\alpha) \cdot n_1.$$

Wenn hierbei $n_1 = +1$ ist, so ist die Richtigkeit des Satzes evident; man kann nun bei den weiteren Untersuchungen einfach wieder annehmen, daß n_1 eine ganze rationale Zahl ohne quadratische Faktoren ist, für welche nach den allgemeinen Sätzen über die Normenreste die Gleichung besteht:

$$\left(\frac{n_1,\, m}{p}\right) = +1,$$

für *alle* Primzahlen p. Hiermit ist aber die folgende wichtige Tatsache gewonnen: wenn der Satz bewiesen ist für ein beliebiges m und für alle Zahlen $|n_1| \leq |\sqrt{d}|$, so gilt derselbe auch allgemein für jedes n; denn es läßt sich ja dieser letztere allgemeine Fall auf jenen speziellen zurückführen.

Es ist daher keine Beschränkung, wenn man voraussetzt, daß $|n_1| \leq |\sqrt{d_m}|$ ist, indem d_m die Diskriminante des Körpers $k(\sqrt{m})$ bezeichnen möge. Nimmt man an, der Satz sei richtig für die beiden Zahlen n_1 und m, dann ist also $n_1 = \frac{x^2 - my^2}{u^2 - mv^2}$. Hierin können offenbar x, y oder u, v nicht zugleich Null sein, dasselbe gilt von x, u und von y, v, weil n_1 sonst eine, ev. sogar gebrochene, Quadratzahl wäre. Somit kann man die letzte Gleichung nach m auflösen und erhält:

$$m = \frac{x^2 - n_1 u^2}{y^2 - n_1 v^2}.$$

Weil nun nach dem Vertauschungssatz für das Hilbertsche Symbol stets:

$$\left(\frac{n_1,\, m}{p}\right) = \left(\frac{m,\, n_1}{p}\right)$$

ist, so kann man den Inhalt der letzten Gleichung auch so aussprechen: wenn der Satz besteht für zwei Zahlen n_1 und m, so ist er auch richtig nach Vertauschung dieser Zahlen, also für m und n_1,

wo aber nun $|n_1| \leqq |\sqrt{d_m}|$ ist. Auch die Umkehrung dieser Behauptung ist richtig.

Ist hierbei $|m| \geqq 4$, so wird $|\sqrt{d_m}| < |m|$ und folglich auch $|n_1| < |m|$.

Nun ist aber nach der zuerst gefundenen Tatsache der Satz richtig für m und n_1 (wo $|n_1| \leqq |\sqrt{d_m}|$), falls er für zwei Zahlen m_1, n_1 gilt, von denen $|m_1| \leqq |\sqrt{d_{n_1}}|$ ist. Somit ist der Beweis für zwei beliebige Zahlen n, m auf den Beweis für zwei neue Zahlen $\bar{n} = m_1$ und $\bar{m} = n_1$ zurückgeführt, die absolut genommen kleiner sind als $|m|$, solange $|\sqrt{d_m}| \leqq |m|$, d. h. solange $|m| \geqq 4$ ist.

Da man alsdann rückwärts von der Gültigkeit des Satzes für die zwei Zahlen $\bar{n}$, $\bar{m}$ auf die Gültigkeit des Satzes für die absolut genommen größeren Zahlen n, m schließen darf, so ist der Satz bewiesen, wenn seine Richtigkeit für die Körper $k(\sqrt{-1})$, $k(\sqrt{\pm 2})$, $k(\sqrt{\pm 3})$ nachgewiesen ist, für welche $|m| < 4$ ist.

Alle diese Körper haben die Klassenanzahl $h = 1$. Man ersieht daher aus einer ähnlichen Betrachtung, wie sie zu Anfang des Beweises angestellt wurde, daß das Ideal (n) im Körper $k(\sqrt{m})$ zerfällt, falls n eine ganze Zahl ist, für welche $\left(\frac{n,\, m}{p}\right) = +1$ ausfällt für *alle* Primzahlen p. Dann ist aber n auch die Norm einer ganzen Zahl des Körpers, weil nämlich für die imaginären Körper von vornherein n positiv ist, weil ferner im Körper $k(\sqrt{2})$ die Grundeinheit ε die Norm -1 besitzt und weil endlich im Körper $k(\sqrt{3})$ nur dann stets $\left(\frac{n,\, m}{3}\right) = +1$ ist, wenn für eine zu 3 prime Zahl n: $\left(\frac{+n}{3}\right) = 1$ und für $n = 3n_1$:

$$\left(\frac{-n_1}{3}\right) = +1$$

ist, wonach $+n \equiv x^2\ (3)$ oder $n = x^2 - 3y^2$ und analog $3n_1 = 9x^2 - 3y^2$ werden muß. Der Satz gilt also für die angeführten speziellen Körper, folglich gilt er allgemein; ferner sieht man leicht, daß die Formulierung des Satzes so erweitert werden kann, daß darin n irgend eine ganze rationale Zahl bedeutet.

Zur Erläuterung mögen noch einige Zahlenbeispiele angeführt werden. Man findet für *alle* Primzahlen p:

1.) Im Körper $k(\sqrt{-1})$:

$$\left(\frac{+1,\, -1}{p}\right) = +1 \quad \text{und} \quad \left(\frac{2,\, -1}{p}\right) = +1,$$

und andererseits ist:

$$1 = n(-1), \quad 2 = n(1 + \sqrt{-1}).$$

2.) Im Körper $k(\sqrt{2})$:

$$\left(\frac{\pm 1,\ 2}{p}\right) = +1 \quad \text{und} \quad -1 = n(\varepsilon),$$

wo $\varepsilon = 1 + \sqrt{2}$ die Grundeinheit des Körpers ist,

$$\left(\frac{\pm 2,\ 2}{p}\right) = +1 \quad \text{und} \quad 2 = n[\sqrt{2}(1+\sqrt{2})],$$
$$\text{bezw. } -2 = n(\sqrt{2}).$$

3.) Im Körper $k(\sqrt{-2})$:

$$\left(\frac{1,\ -2}{p}\right) = +1 \quad \text{und} \quad 1 = n(-1),$$

$$\left(\frac{2,\ -2}{p}\right) = +1 \quad \text{und} \quad 2 = n(\sqrt{-2}).$$

4.) Im Körper $k(\sqrt{3})$:

$$\left(\frac{1,\ 3}{p}\right) = +1 \quad \text{und} \quad 1 = n(-1),$$

$$\left(\frac{-2,\ 3}{p}\right) = +1 \quad \text{und} \quad -2 = n(1+\sqrt{3}).$$

5.) Im Körper $k(\sqrt{-3})$:

$$\left(\frac{\pm 1,\ -3}{p}\right) = +1 \quad \text{und} \quad 1 = n(-1).$$

6.) Im Körper $k(\sqrt{7})$:

$$\left(\frac{2,\ -7}{p}\right) = +1 \quad \text{und} \quad 2 = \frac{1}{4} + 7\,\frac{1}{4}\cdot$$

In diesen Beispielen sind nochmals alle Zahlenpaare n, m berücksichtigt, für welche $|n| < |\sqrt{d_m}|$ ist.

Satz. *Jede Klasse des Hauptgeschlechtes in einem quadratischen Zahlkörper $k(\sqrt{m})$ läßt sich durch das Quadrat einer Klasse des Körpers darstellen.*

Beweis. Es sei $\mathfrak{h}$ ein Ideal, das einer Klasse des Hauptgeschlechtes angehört. Dann ist die Bedingung erfüllt, daß

$$\left(\frac{\pm n(\mathfrak{h}),\ m}{p}\right) = +1$$

ist für *alle* Primzahlen p. Nach dem eben bewiesenen Hilfssatz ist also

$$\pm n(\mathfrak{h}) = n(\alpha),$$

wo α eine ganze oder gebrochene Zahl des Körpers $k(\sqrt{m})$ bedeutet. Man setze nun $\frac{\mathfrak{h}}{(\alpha)} = \frac{\mathfrak{j}}{\mathfrak{j}_1}$, gleich dem Quotienten zweier Ideale, welche relativ prim zueinander sind. Wenn $\mathfrak{j}$ und $\mathfrak{j}_1$ teilerfremd sind, so sind auch die konjugierten Ideale $\mathfrak{j}'$ und $\mathfrak{j}_1'$ teilerfremd.

Nun ist

$$n\left(\frac{\mathfrak{h}}{\alpha}\right) = \pm 1 = \frac{\mathfrak{j}\mathfrak{j}'}{\mathfrak{j}_1\mathfrak{j}_1'}, \quad \text{oder} \quad \mathfrak{j}\mathfrak{j}' = \mathfrak{j}_1\mathfrak{j}_1'.$$

Diese Relation kann aber wegen der Voraussetzung über die Ideale $\mathfrak{j}$ und $\mathfrak{j}_1$ nur stattfinden, wenn $\mathfrak{j} = \mathfrak{j}_1'$ und $\mathfrak{j}_1 = \mathfrak{j}'$ ist. Alsdann ist

$$\mathfrak{h} = \frac{\alpha}{n(\mathfrak{j})}\mathfrak{j}^2 \quad \text{oder} \quad \mathfrak{h} \sim \mathfrak{j}^2.$$

Bezeichnet H die Klasse, welcher $\mathfrak{h}$ angehört, und K die Klasse, welcher $\mathfrak{j}$ angehört, so gilt die entsprechende Beziehung:

$$H = K^2,$$

wie es der Satz verlangt.

Auf Grund der bisher entwickelten Sätze läßt sich nun endlich der Existenzbeweis für die Geschlechter erbringen.

Satz. *Die Anzahl der in dem quadratischen Zahlkörper $k(\sqrt{m})$ vorhandenen Geschlechter ist gleich 2^{r-1}.*

Beweis. Die Klassenanzahl des Körpers sei h, die Anzahl der Geschlechter g, und ferner sei f die Anzahl der Klassen, welche jedes Geschlecht enthält, dann ist:

$$h = g \cdot f.$$

Es mögen nun die Klassen des Hauptgeschlechts mit

$$H_1, H_2, \ldots H_f$$

bezeichnet sein, so kann man stets f Klassen K_1, K_2 usw. angeben, so daß jedesmal eine Identität stattfindet:

$$H_1 = K_1^2, \quad H_2 = K_2^2, \ldots, \quad H_f = K_f^2,$$

wobei also die Klassen K_1^2, $K_2^2 \ldots$ lauter verschiedene Klassen bezeichnen.

Sind $A_1, A_2, \ldots A_a$ die sämtlichen $a = 2^{r-1}$ verschiedenen ambigen Klassen des Körpers, so kann man zunächst zeigen, daß durch:

$$\begin{array}{c} K_1A_1,\ K_1A_2,\ \ldots\ K_1A_a \\ \cdots\cdots\cdots \\ K_fA_1,\ K_fA_2,\ \ldots\ K_fA_a, \end{array}$$

alle Klassen des Körpers und jede nur einmal dargestellt wird. Diese Klassen sind nämlich alle verschieden voneinander, denn wenn etwa:

$$K_\lambda A_\mu = K_\nu A_\varrho$$

wäre, so müßte auch:

$$K_\lambda^2 = K_\nu^2$$

sein, was der Konstruktion der Klassen K widersprechen würde. Ist

andererseits C irgend eine Klasse des Körpers, so gehört C^2 sicher dem Hauptgeschlecht an, und es muß für ein bestimmtes i und K_i:

$$C^2 = K_i^2$$

sein. Die Klasse $\frac{C}{K}$ ist dann aber eine ambige Klasse und folglich darf man $C = AK$ ansetzen, so daß C in der Tat unter den aufgestellten Idealklassen schon enthalten ist.

Es ist daher einerseits $h = gf$ und andererseits $h = a \cdot f = 2^{r-1}f$, also wird notwendig:

$$g = 2^{r-1}.$$

Da nun früher gezeigt wurde, daß das Produkt der Einheiten eines Charakterensystems für ein Geschlecht $+1$ sein muß und danach *höchstens* 2^{r-1} verschiedene Geschlechter existieren, so folgt zum Schluß, daß ein System von r Einheiten ± 1 sicher dann, aber auch nur dann, das Charakterensystem für ein Ideal des Körpers $k(\sqrt{m})$ darstellt, wenn das Produkt der r Einheiten gleich $+1$ ist.

Aus dem Satz von der Existenz der Geschlechter lassen sich eine Reihe interessanter Folgerungen ziehen, worauf wir nun eingehen.

32. Anwendungen des Existenzsatzes der Geschlechter.

1.) Wenn die Klassenanzahl eines Körpers ungerade ist, so gehören alle Klassen zu einem und demselben Geschlecht.

Denn es ist

$$h = 2^{r-1} \cdot f = g \cdot f;$$

wenn also h ungerade ist, so muß $g = 2^{r-1} = 1$ sein.

Einige weitere Folgerungen ergeben sich durch die Untersuchung spezieller Körper $k(\sqrt{m})$.

2.) Es sei $m = p$ eine positive oder negative Primzahl und $m \equiv 1, (4)$. Dann ist $d = m$, $t = 1$, $r = t = 1$. Die Anzahl der Geschlechter ist $2^0 = 1$. Der Körper enthält nur ein ambiges Hauptideal und nur eine ambige Klasse, die Hauptklasse. Wie früher schon gezeigt wurde, ist die Klassenanzahl des Körpers h ungerade und im Falle eines reellen Körpers die Norm der Grundeinheit gleich -1.

3.) Es sei $m = p$ eine positive Primzahl von der Form $4n + 3$. Dann ist $d = 4p$, $l_1 = 2$, $l_2 = p$, also $t = 2$. Das Charakterensystem von -1 wird:

$$\left(\frac{-1, p}{2}\right) = -1, \quad \left(\frac{-1, p}{p}\right) = -1,$$

somit ist $r = t - 1 = 1$. Die Anzahl der ambigen Klassen, sowie die

Anzahl der Geschlechter wird also $2^0 = 1$. Somit ist insbesondere $\mathfrak{l}_1 = (2, 1 + \sqrt{p})$ ein ambiges Hauptideal, d. h. aber, es muß die Diophantische Gleichung

$$\pm 2 = x^2 - py^2$$

stets in *ganzen Zahlen lösbar sein*, und zwar kann man zum voraus angeben, daß nur die Gleichung:

$$+ 2 = x^2 - py^2 \quad \text{für} \quad p = 8n + 7$$
$$- 2 = x^2 - py^2 \quad \text{für} \quad p = 8n + 3$$

lösbar ist.

Die Lösung solcher Gleichungen gelingt meist rasch durch Probieren. Häufig kommt man schnell zum Ziel, ähnlich wie im Fall der Gleichung $\pm 1 = x^2 - my^2$, wenn man zuerst die Wurzeln der Kongruenz sucht:

$$x^2 \mp 2 \equiv 0, \ (p).$$

Sei w eine Lösung dieser Kongruenz, so ist der gesuchte Wert x sicher unter den Zahlen $x = w + p\lambda$ enthalten, wo λ eine positive oder negative ganze Zahl ist. Man kann nun für λ Werte einsetzen und nachsehen, wann $\frac{x^2 \mp 2}{p}$ ein Quadrat ist, oder man probiert, für welche Werte von λ:

$$\frac{w^2 \mp 2}{p} + 2w\lambda + p\lambda^2 = y^2$$

d. h. eine Quadratzahl wird.

4.) Es sei $m = -p$ eine negative Primzahl von der Form $m \equiv 3, (4)$, dann hat man $r = t = 2$ zu setzen. Die Klassenanzahl h ist *gerade*, und der Körper enthält zwei ambige Klassen mit ambigen Idealen.

Die ambigen Primideale sind:

$$\mathfrak{a} = (\sqrt{m}) \quad \text{und} \quad \mathfrak{b} = (2, 1 + \sqrt{m}).$$

wo nun $\mathfrak{b} \nsim 1$ ist. Wird $n(\mathfrak{a}) = \bar{n} = -m$ und $n(\mathfrak{b}) = \bar{n}_1 = +2$ gesetzt, so erhält man für $\mathfrak{a}$ und $\mathfrak{b}$ in $k(\sqrt{m})$ die Charakterensysteme:

$$\left(\frac{-m, m}{2}\right) = +1, \quad \left(\frac{-m, m}{m}\right) = +1,$$
$$\left(\frac{2, m}{2}\right) = \pm 1, \quad \left(\frac{2, m}{m}\right) = \pm 1,$$

wobei in der letzten Reihe gleichzeitig die oberen oder die untern Zeichen gelten, je nachdem $+p \equiv \begin{cases} 1 \\ 5 \end{cases}, (8)$ ist. Gelten die beiden oberen (Plus-)Zeichen, so gehört auch die durch $\mathfrak{b}$ bestimmte Klasse B zum Hauptgeschlecht. Da aber jede Klasse des Hauptgeschlechtes sich durch das Quadrat einer andern Klasse darstellen läßt, so kann

$$B = K^2$$

gesetzt werden, da ferner $B^2 = 1$, also auch $K^4 = 1$ ist, so ist die Klassenanzahl des Körpers in diesem Fall durch 4 teilbar, d. h. mindestens gleich 4. Gelten die unteren Zeichen, so kann B sicher nicht gleich dem Quadrat einer Klasse sein, und die Klassenanzahl ist alsdann nur durch 2, aber keine höhere Potenz von 2 teilbar.

Sind für diesen Fall $H_1, H_2, \ldots H_f$, die Klassen des Hauptgeschlechts, wo f eine ungerade Zahl bedeutet, so sind die übrigen Klassen:

$$H_1 B, \quad H_2 B, \ldots \quad H_f B,$$

und es gelten wegen $B^2 = 1$ die Relationen:

$$H_\lambda = H_\mu^{\,2}, \quad H_\lambda = H_\nu H_\iota,$$

wo λ, μ, ν, ι Zahlen der Reihe 1 bis f sind.

5.) Es sei $m = p \cdot p_1$ eine positive Zahl und p, p_1 beides positive Primzahlen von der Form $4n + 1$. Dann ist $t = 2$, $r = t$, $g = 2^1 = 2$. Die Anzahl der ambigen Klassen und der Geschlechter ist 2, die Klassenanzahl gerade.

Die ambigen Ideale sind nun:

$$(p, \sqrt{m}); \quad (p_1, \sqrt{m}); \quad (\sqrt{m}).$$

Falls die Norm der Grundeinheit ε: $n(\varepsilon) = +1$ ist, enthält der Körper eine ambige Klasse, welche kein ambiges Ideal enthält; dann müssen aber die drei angeschriebenen Ideale alle Hauptideale sein, d. h. es müssen die Gleichungen

$$\pm p = \left(x + \frac{y}{2}\right)^2 - \frac{p p_1}{4} y^2$$

$$\pm p_1 = \left(x_1 + \frac{y_1}{2}\right)^2 - \frac{p p_1}{4} y_1^{\,2}$$

in ganzen Zahlen lösbar sein. Setzt man $x + \frac{y}{2} = \frac{z}{2} p$, so folgt, daß auch die Gleichung

$$\pm 1 = p\left(\frac{z}{2}\right)^2 - p_1\left(\frac{y}{2}\right)^2$$

in ganzen Zahlen lösbar sein muß.

Wenn umgekehrt diese Gleichungen in ganzen Zahlen lösbar sind, so ist die Norm der Grundeinheit $+1$.

Für die Lösbarkeit der Diophantischen Gleichung ist offenbar eine notwendige Bedingung, daß $\left(\frac{p}{p_1}\right) = +1$ ist, und man erhält den Satz:

Satz. *Die Norm der Grundeinheit des reellen Körpers $k(\sqrt{m})$, für welchen $m = pp_1$ das Produkt zweier positiver Primzahlen von der Form $4n+1$ ist, ist sicher dann gleich -1, wenn $\left(\frac{p}{p_1}\right) = -1$ ist.*

Wenn $\left(\frac{p}{p_1}\right) = \left(\frac{p_1}{p}\right) = +1$ ist, so kann die Grundeinheit ε die Norm ± 1 besitzen, wie man an den Körpern $k(\sqrt{145})$ (wo $\varepsilon = 11 + 2\omega$ und $n(\varepsilon) = -1$ ist) und $k(\sqrt{221})$ (wo $\varepsilon = 7 + \omega$ und $n(\varepsilon) = +1$ ist) sieht.

Die Frage, wann in diesem Fall $n(\varepsilon) = -1$ und wann $n(\varepsilon) = +1$ ausfällt[1]) kann hier nicht weiter erörtert werden, doch lassen sich noch besondere Sätze aufstellen; z. B. wenn $\left(\frac{p}{p_1}\right) = +1$ ist, und $k(\sqrt{pp_1})$ die Klassenanzahl 2 besitzt, so ist die Norm der Grundeinheit $+1$.

Das Ergebnis kann auch so gefaßt werden, daß man sagt: von den beiden Gleichungen:

$$-1 = \left(x + \frac{y}{2}\right)^2 - \frac{pp_1}{4} y^2 \qquad (1)$$

und:

$$\pm 1 = p\left(\frac{z}{2}\right)^2 - p_1\left(\frac{y}{2}\right)^2 \qquad (2)$$

ist immer eine und nur eine in ganzen Zahlen lösbar.

Beide Gleichungen ließen sich auch benützen, um eine Aussage zu machen über die Genauigkeit angenäherter Darstellungen von $\sqrt{\frac{p}{p_1}}$ oder $\sqrt{pp_1}$ durch rationale Brüche.

Ähnliche Resultate, wie die bisherigen, lassen sich entwickeln für den Fall, daß $p = 2$ und $p_1 \equiv 1$, (4) ist.

6.) Es sei $m = qq_1$ eine positive Zahl, deren Teiler q, q_1 Primzahlen von der Form $4n+3$ sind. Dann ist $m \equiv 1$, (4), $t = 2$, $r = t - 1 = 1$, also $g = 2^0 = 1$. Die Klassenanzahl ist ungerade, da alsdann die ambigen Ideale sämtlich Hauptideale sein müssen und keine ambige Klasse ohne ambiges Ideal im Körper existieren kann. Die Äquivalenz:

$$(q, \sqrt{qq_1}) \sim 1,$$

ist gleichbedeutend mit dem Satz, daß stets eine von den beiden Gleichungen:

---

1) Weiteres hierüber siehe bei P. G. Lejeune-Dirichlet, Ges. Werke, Bd. I: Einige neue Sätze über unbestimmte Gleichungen; S. 288, wo diese Frage auf anderem Wege weiter behandelt ist.

$$\pm 4 = qx^2 - q_1 y^2$$

in ganzen rationalen Zahlen x, y lösbar ist, und zwar ist die Gleichung mit dem oberen oder unteren Vorzeichen lösbar, je nachdem:

$$\left(\frac{q}{q_1}\right) = +1 \quad \text{oder} \quad \left(\frac{q}{q_1}\right) = -1$$

ausfällt.[1])

7.) Ist $m = \pm pq$ eine positive oder negative Zahl, und $p \equiv 1$, (4), $q \equiv 3$, (4), so ist $t = 3$ resp. $t = 2$, $r = 2$ und $g = 2$, die Klassenanzahl des Körpers also sicher gerade.

Aus den bisherigen Spezialfällen stellen wir nun noch folgenden Satz zusammen[2]):

Satz. *Die Klassenanzahl eines Körpers* $k(\sqrt{m})$ *ist ungerade:* 1.) *wenn* m *eine positive oder negative Primzahl und* $m \equiv 1$, (4) *ist,* 2.) *wenn* m *eine positive Primzahl* q, *von der Form* $4n + 3$ *ist,* 3.) *wenn* $m = qq_1$ *eine positive Zahl, das Produkt zweier positiver Primzahlen von der Form* $4n + 3$ *ist. In diesen und nur in diesen Fällen kann die Klassenanzahl des Körpers* $h = 1$ *sein; in allen andern Fällen ist die Klassenanzahl des Körpers eine gerade Zahl.*

33. Zahlringe.

Anhangsweise soll hier noch ein Begriff erläutert werden, welcher sehr wichtig ist, und von welchem später auch eine Anwendung gemacht werden muß: der Begriff des *Zahlrings* in einem Zahlkörper.[3])

1) Wenn eine Lösung der Gleichung $\pm 4 = qx^2 - q_1 y^2$ bekannt ist, so kann man mit Hilfe der Einheiten des reellen Körpers $k(\sqrt{qq_1})$ unendlich viele andere Lösungen daraus entwickeln. Man kann übrigens auch beweisen, daß die Gleichungen $\pm 1 = qx^2 - q_1 y^2$ lösbar sind, je nachdem $\left(\frac{q}{q_1}\right) = \pm 1$ ist.

2) Ich übergehe in diesen Folgerungen aus dem Existenzsatz der Geschlechter eine Reihe leicht abzuleitender *negativer* Aussagen über die Nichtauflösbarkeit von Gleichungen u. a.

3) Der Name Zahlring rührt m. W. von Herrn Hilbert her. (Hilbert, Zahlb. Kap. IX.) Herr Dedekind gebraucht im Anschluß an die Nomenklatur von Gauß das Wort *„Ordnung"*. Vgl.: Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers, Festschr. zur Säkularf. des Geburtstages von C. F. Gauß. Braunschweig 1877, S. 15. Die Bezeichnung *„Integritätsbereich"* hat Kronecker eingeführt, s. Ges. Werke, Bd. II. Grundzüge einer arithmet. Theorie usw. S. 260 § 5.

Sind zum Beispiel $\alpha, \beta, \gamma \ldots$ beliebige *ganze* Zahlen des Körpers $k(\sqrt{m})$, so sagt man, daß die Gesamtheit aller Zahlen, welche sich aus den angeschriebenen Zahlen und den ganzen rationalen Zahlen durch die beliebig oft angewendeten Operationen der Addition, Subtraktion und Multiplikation ableiten lassen, oder m. a. W. die sämtlichen rationalen ganzen Funktionen der $\alpha, \beta, \gamma \ldots$ mit ganzen rationalen Koeffizienten einen *Zahlring* oder *Ring* oder *Integritätsbereich* des Körpers $k(\sqrt{m})$ bilden. Es gibt unendlich viele Zahlringe in einem Körper, und der Körper selbst ist der umfassendste dieser Ringe.

Es genügt für uns, die Eigenschaften der Zahlringe in einem ganz speziellen Fall zu studieren, der sich bei unseren Entwicklungen sozusagen aufdrängt.

Wenn m eine ganze Zahl und $m \equiv 1, (4)$ ist, so findet man bekanntlich für den Körper $k(\sqrt{m})$ als Basiszahl $\omega = \frac{1+\sqrt{m}}{2}$. Es liegt nahe, nach den Änderungen zu fragen, die sich ergeben, wenn man statt des Körpers $k(\sqrt{m})$ nur den durch $1, \sqrt{m}$ bestimmten Zahlring betrachtet.

Der durch $1, \sqrt{m}$ bestimmte Zahlring soll stets mit $r(\sqrt{m})$ oder, wenn keine Zweideutigkeit entstehen kann, mit r bezeichnet werden.

Ohne weiteres sieht man die folgenden Tatsachen ein:

1.) Jede Zahl des Zahlrings $r(\sqrt{m})$ ist zugleich eine ganze Zahl des Körpers $k(\sqrt{m})$.

2.) Jede Zahl des Rings ist in der Form $a + b\sqrt{m}$ darstellbar, wo a, b ganze rationale Zahlen bedeuten.

Die Zahlen $1, \sqrt{m}$ bilden eine *Basis* des Rings.

3.) Wenn ω_1, ω_2 und ω_1^*, ω_2^* zwei verschiedene Zahlenpaare sind, welche je eine Basis des Rings r bilden, so gibt es stets vier ganze rationale Zahlen r, s, t, u mit der Bedingung $ru - st = \pm 1$ so daß:

$$\omega_1^* = r\omega_1 + s\omega_2, \quad \omega_2^* = t\omega_1 + u\omega_2,$$

wird.

Der Ausdruck:

$$d_r = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m,$$

oder allgemeiner geschrieben:

$$d_r = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2,$$

heißt die Diskriminante des Zahlrings. Dieselbe ist also stets ein Vielfaches der Körperdiskriminante.

Fast wörtlich überträgt sich die Definition des Körperideals auf den Zahlring:

Man versteht unter einem **Ringideal** irgend ein System von unbegrenzt vielen Zahlen des Zahlrings:

$$\mathfrak{j}_r = (\alpha, \beta, \gamma, \ldots \lambda_1\alpha + \lambda_2\beta + \lambda_3\gamma + \cdots, \cdots),$$

welches die Eigenschaft hat, daß jede lineare Kombination irgend welcher Zahlen $\alpha, \beta, \gamma, \ldots$ des Systems mit Zahlen $\lambda_1, \lambda_2, \lambda_3 \ldots$ des Rings wiederum dem System angehört.

Es ist klar, insbesondere für den speziellen hier betrachteten Fall, daß auch die Begriffe: *Basis* eines Ideals, *Kongruenzen* nach einem Ideal, *Norm* eines Ideals, *konjugiertes Ideal*, *Produkt* zweier Ideale, sich ohne weiteres auf das Ringideal übertragen lassen.

Wenn z. B. $\mathfrak{j}_r = (\alpha, \beta, \gamma \ldots)$ ist, und i den größten gemeinsamen Teiler aller rationalen Zahlen des Ideals bedeutet, ferner wenn $\alpha = a + b\sqrt{m}$ usw. gesetzt wird und i_2 den größten gemeinsamen Teiler aller Koeffizienten b bezeichnet, so ist eine Basis des Ringideals stets von der Art: $i,\ i_1 + i_2\sqrt{m}$, wo $i_1^2 - i_2^2 m \equiv 0,\ (i)$ sein muß. Ferner ist $n(\mathfrak{j}_r) = i i_2$.

Man kann jedoch nicht ohne weiteres alle Sätze, welche für Ideale des Körpers gelten, auf die Ringideale übertragen. So ist z. B. im Zahlring $r(\sqrt{-3})$ des Körpers $k(\sqrt{-3})$ die Zahl 4 auf doppelte Weise zerlegbar:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

ohne daß im Zahlring $r(\sqrt{-3})$ einer der Faktoren $1 + \sqrt{-3}$ oder $1 - \sqrt{-3}$ durch 2 teilbar wäre. Es existiert weder eine Identität

$$1 + \sqrt{-3} = 2 \cdot (a + b\sqrt{-3}),$$

wo a, b ganze rationale Zahlen sind, noch eine andere:

$$2 = (1 + \sqrt{-3})(a + b\sqrt{-3}).$$

Wollte man nun, wie es in einem früheren Beispiel geschehen ist, zur Herstellung der eindeutigen Zerlegbarkeit derart verfahren, daß man die Ideale

$$\mathfrak{j} = (2,\ 1 + \sqrt{-3}),\quad \mathfrak{j}' = (2,\ 1 - \sqrt{-3})$$

aufstellt, so führt auch dieser Weg nicht mehr zum Ziel. Während z. B. im *Körper* $k(\sqrt{-3})$ das Produkt der konjugierten Körperideale $\mathfrak{j}\cdot\mathfrak{j}'$ ein Hauptideal ist, so ist im Zahlring:

$$\mathfrak{j}\mathfrak{j}' = (4, 2+2\sqrt{-3}, 2, -2\sqrt{-3}, 4\sqrt{-3}, \ldots) = (2)\cdot(2, 1+\sqrt{-3}),$$

also kein Hauptideal.

In der Tat nimmt das Ringideal $(2, 1+\sqrt{-3})$ eine besondere Stellung ein. Im Körper $k(\sqrt{-3})$ ist dasselbe ein Hauptideal, gleich (2), und man kann das Ideal gewissermaßen als ein uneigentliches Hauptideal des Zahlrings betrachten. Jedenfalls zeigt das Beispiel der Zerlegung von 4 schon, daß selbst für die Ringideale der Satz von der eindeutigen Zerlegbarkeit nicht unbeschränkt gelten kann.

Im allgemeinen ist ein Ideal des Körpers nicht zugleich ein Ringideal, jedoch gibt es selbstverständlich unendlich viele Körperideale, welche gleichzeitig Ringideale sind. Der größte gemeinsame Teiler aller Körperideale, welche zugleich Ringideale sind (für den speziellen Fall $k(\sqrt{m})$ das Ideal (2)), heißt der *Führer* des Rings.

Satz. *Ein Körperideal* $\mathfrak{j}$ *ist dann und nur dann zugleich ein Ringideal, wenn dasselbe durch das Ideal* (2) *teilbar ist.*

Beweis. Falls $\mathfrak{j}$ ein durch 2 teilbares Körperideal und $\mathfrak{j} = (2)\mathfrak{j}_1$ ist, so enthält $\mathfrak{j}$ sicher nur Zahlen des Rings von der Form $2a$ oder $a + b\sqrt{-3}$ und ist also selbst ein Ringideal.

Wenn ferner das Körperideal $\mathfrak{j} = (a, b + c\sqrt{m})$ zugleich Ringideal sein soll, so muß a gerade sein, weil sonst die in $\mathfrak{j}$ enthaltene Zahl $a\cdot\omega = a\frac{1+\sqrt{m}}{2}$ nicht im Ring enthalten wäre, und ebenso muß $b - c$ gerade sein, sonst würde die Zahl $(b-c)\omega' + c\frac{1-m}{2}$ nicht im Ring enthalten sein können. Sind aber a und $b - c$ gerade, so ist $\mathfrak{j}$ durch (2) teilbar.

Aus diesem Satz folgt jetzt unmittelbar, daß das Ideal (2) der Führer des Rings $r(\sqrt{m})$ ist.

Um nun die folgenden Ausführungen möglichst einfach gestalten zu können, führe ich noch einige von Herrn Hilbert gebrauchte Bezeichnungen ein:

Wenn $\mathfrak{j}_r = (\alpha, \beta, \ldots)$ irgend ein Ringideal ist und $\mathfrak{j} = (\alpha, \beta, \ldots)$ den größten gemeinschaftlichen Teiler der Zahlen $\alpha, \beta, \ldots$ im Körper $k(\sqrt{m})$, also ein Körperideal bezeichnet, so heißt $\mathfrak{j}$ das dem Ringideal $\mathfrak{j}_r$ *zugeordnete Ideal.* Ist insbesondere $\mathfrak{j}$ prim zum Führer des

Rings, hier speziell also zum Ideal (2), so heißt $\mathfrak{j}_r$ ein *reguläres Ringideal.*[1])

Zunächst läßt sich nun zeigen, daß die einfachen Teilbarkeitsgesetze, wie sie für die Körperideale gelten, auch für die *regulären* Ringideale richtig sind, wenn man das Produkt und die Division zweier Ringideale ganz analog definiert wie für Körperideale. Es genügen dazu folgende Sätze:

Satz. *Wenn $\mathfrak{j}$ ein Ideal des Körpers $k(\sqrt{m})$ ist, welches prim ist zu (2), so existiert im Ring $r(\sqrt{m})$ stets ein reguläres Ideal $\mathfrak{j}_r$, welchem das Ideal $\mathfrak{j}$ zugeordnet ist.*

Beweis. Es sei $\mathfrak{j}$ ein Körperideal:

$$\mathfrak{j} = (a,\ b + c\omega)$$

und a, $b + c\omega$ die Basiszahlen des Ideals. Falls $\mathfrak{j}$ prim ist zu (2), muß sicher a und folglich auch c ungerade sein. Dann wird

$$\mathfrak{j}_r = (a,\ 2b + 2c\omega)$$

ein Ringideal, dem das Ideal $\mathfrak{j}$ zugeordnet ist. In der Tat ist das dem Ideal $\mathfrak{j}_r$ zugeordnete Ideal $\mathfrak{j} = (a,\ 2b + 2c\omega) = (a,\ b + c\omega)$, weil nämlich

$$-a(b + c\omega) + \frac{a+1}{2}(2b + 2c\omega) = b + c\omega$$

1) Durch die Einführung dieses Begriffes wird nun eigentlich die Untersuchung so modifiziert, daß man überhaupt nur diejenigen Ringideale betrachtet, welche zum Führer $f = 2$ prim sind. Dies ist notwendig. In der Tat zeigte schon die einfache Betrachtung über das Ideal (2) oder $(2,\ 1 + \sqrt{-3})$ auf der vorhergehenden Seite, daß die Zerlegung aller durch 2 teilbaren Zahlen des Ringes zu Widersprüchen führt. Andererseits werden nachher bei der Definition der Äquivalenz regulärer Ringideale Quotienten von ganzen Zahlen eingeführt. Wenn diese gebrochenen Zahlen auch keine eigentliche Bedeutung *für sich* haben, so steht ihre Benützung doch im Widerspruch zu der Definition des Ringes, welche nur *ganze* Zahlen zuläßt. Um diese Schwierigkeiten zu vermeiden, hat Herr Fueter die folgende, wesentlich neue Definition des Ringes in einem Körper eingeführt:

Definition. Alle (ganzen und gebrochenen) Zahlen des Körpers $k(\sqrt{m})$, welche zum Führer $f = 2$ prim sind, oder welche dem Führer f nach der rationalen Zahl 1 kongruent sind, bilden einen *Ring* (Zahlstrahl) des Körpers. (Vgl. Crelles Journal, Bd. 130, S. 208 und: Der Klassenkörper der quadr. Körper und die komplexe Multiplikation. Diss. Göttingen 1903, S. 5, Anmerk.)

So dient der Ring zur Erweiterung der Begriffe der Ideale und der Äquivalenz der Ideale. Addition existiert dagegen nicht im Ring. Diese Definition paßt sich den Anwendungen der Zahlentheorie auf die höhere Algebra gut an. Man erkennt unschwer die Änderungen, welche die obigen Ausführungen auf Grund der neuen Definition erfahren müssen.

eine Zahl des Körpers ist, welche dem Ideal $\mathfrak{j}$ angehört, da $\frac{a+1}{2}$ eine ganze rationale Zahl ist. Da ferner a prim ist zum Führer (2), so ist $\mathfrak{j}_r$ ein *reguläres* Ringideal.

Satz. *Dem Produkt zweier regulärer Ringideale ist das Produkt der zugeordneten Körperideale zugeordnet.*

Beweis. Wenn wie im vorhergehenden Beweis

$$\mathfrak{j} = (a,\, b + c\omega), \quad \mathfrak{h} = (a_1,\, b_1 + c_1\omega)$$

zwei den regulären Ringidealen $\mathfrak{j}_r$ und $\mathfrak{h}_r$ zugeordnete Körperideale sind, so ist

$$\mathfrak{j} \cdot \mathfrak{h} = (aa_1,\, a_1 b + a_1 c\omega,\, ab_1 + ac_1\omega,\, \ldots)$$

dem Produkt der regulären Ringideale:

$$\mathfrak{j}_r \mathfrak{h}_r = (aa_1,\, a_1 2b + a_1 c + a_1 c\sqrt{m},\, a2b_1 + ac_1 + ac_1\sqrt{m},\, \ldots)$$

zugeordnet.

Durch Zusammenfassung dieser beiden Sätze zeigt man, daß jedes *reguläre* Ringideal nur auf eine einzige Weise in ein Produkt aus regulären Ringidealen zerlegt werden kann.

In der Tat, ist $\mathfrak{j}_r$ ein reguläres Ringideal und $\mathfrak{j}$ das zu (2) prime zugeordnete Körperideal, so zerfällt $\mathfrak{j}$ im Körper $k(\sqrt{m})$ in eindeutiger Weise in ein Produkt von Primidealen, die auch ihrerseits alle prim zum Führer (2) sind. Jedem Primfaktor entspricht also ein reguläres Ringideal und dem Produkt dieser letzteren ist wiederum das Ideal $\mathfrak{j}$ zugeordnet. Zu diesem Ideal gehört ja aber nach Voraussetzung das Ringideal $\mathfrak{j}_r$, so daß also das Produkt der regulären Ringideale das gegebene Ideal $\mathfrak{j}_r$ selbst ist.

Die weitere Übertragung der Tatsachen, welche für die Ideale des Körpers gelten, auf den Zahlring ist nun vollends einfach. Es mögen nur noch einzelne Sätze extra angeführt werden:

Die Norm eines regulären Ringideals $n(\mathfrak{j}_r)$ ist gleich der Norm des zugeordneten Körperideals, weshalb die Sätze über Normen analog wie für den Körper bestehen. Ferner:

Zwei reguläre Ringideale $\mathfrak{a}_r$ und $\mathfrak{b}_r$ heißen *äquivalent,* in Zeichen $\mathfrak{a}_r \sim \mathfrak{b}_r$, wenn im Ring zwei ganze Zahlen α, β existieren, so daß $\frac{\mathfrak{a}_r}{\mathfrak{b}_r} = \frac{\alpha}{\beta}$ ist, während zugleich die Norm von $\frac{\alpha}{\beta}$, also $n\left(\frac{\alpha}{\beta}\right)$, positiv ausfällt.[1])

1) Diese engere Fassung des Äquivalenzbegriffes ist notwendig, um große Umständlichkeiten bei den weiteren Untersuchungen zu vermeiden. Man kann die engere Definition der Äquivalenz auch für den Körper selbst zugrunde legen.

Alle äquivalenten Ideale gehören wieder zu einer Idealklasse und man beweist genau wie früher die Endlichkeit der Klassenanzahl.

Der Satz über die *Einheiten* nimmt für den Zahlring folgende Gestalt an:

Satz. *Die Einheiten in einem imaginären Ring* $r(\sqrt{m})$ *sind* ± 1, *dagegen existieren in einem reellen Ring* $r(\sqrt{m})$ *unendlich viele Einheiten, die sich durch eine einzige Grundeinheit* ε_r *in der Form* $\pm \varepsilon_r^e$ *darstellen lassen.*

Beweis. Es ist nur nötig, die Behauptung für reelle Körper und Ringe zu beweisen.

Wenn $\frac{m-1}{4} \equiv 0, (2)$ oder $m \equiv 1, (8)$ ist, und wenn $\varepsilon = a + b\omega$ die Grundeinheit des Körpers $k(\sqrt{m})$ bezeichnet, so folgert man aus der Gleichung:

$$n(\varepsilon) = \pm 1 = a^2 + ab + \frac{1-m}{4} b^2,$$

daß b eine gerade und a eine ungerade Zahl sein muß. Daher ist $\varepsilon = a + \frac{b}{2} + \frac{b}{2}\sqrt{m}$ auch eine Einheit in $r(\sqrt{m})$, man darf $\varepsilon_r = \varepsilon$ annehmen.

Wenn zweitens $\frac{m-1}{4}$ ungerade, $m \equiv 5, (8)$ ist und wieder $\varepsilon = a + b\omega$ die Grundeinheit in $k(\sqrt{m})$ bezeichnet, so folgt aus $n(\varepsilon) = \pm 1$, daß entweder b gerade und a ungerade, oder b ungerade und a gerade oder auch a und b ungerade sein muß.

Im ersten Fall kann man einfach wieder $\varepsilon_r = \varepsilon$ setzen; in den anderen Fällen wird $\varepsilon^3 = B + C\omega$ eine Einheit des Rings, weil $C = 3ab(a+b) + b^3\left(1 + \frac{m-1}{4}\right)$ eine gerade Zahl ist, und es kann $\varepsilon_r = \varepsilon^3$ als Grundeinheit gewählt werden.

Die Norm der Grundeinheit ε_r ist positiv oder negativ, je nachdem $n(\varepsilon) = \pm 1$ ist.

Dadurch hätten sich z. B. die Definition auf S. 140—141 und der Satz auf S. 152 usw. vereinfachen lassen. (Vgl. Hilbert, Zahlber., S. 315 u. 316.) Das Charakterensystem eines Ideals $\mathfrak{j}$ ist dann stets das System der t Einheiten:

$$\left(\frac{\pm n(\mathfrak{j}), m}{l_1}\right) \cdots \left(\frac{\pm n(\mathfrak{j}), m}{l_t}\right).$$

An dieser Stelle fügt sich noch zweckmäßig eine Bemerkung ein über die bisher stets festgehaltene Voraussetzung, daß die Grundzahl m des Körpers $k(\sqrt{m})$ keine quadratischen Faktoren enthalten soll.

Läßt man diese Voraussetzung fallen und ist $m = f^2 \cdot m_1$, so hat man zwei Möglichkeiten: 1.) Man kann *alle* ganzen Zahlen $\frac{a + b\sqrt{m}}{c}$ betrachten; da dann

$$\sqrt{m_1} = \frac{\sqrt{m}}{f} \text{ ev. } \frac{1 + \sqrt{m_1}}{2} = \frac{f + \sqrt{m}}{2f}$$

auch ganze Zahlen sind, so ist in diesem vollen Umfang der Körper $k(\sqrt{m})$ identisch mit $k(\sqrt{m_1})$. 2.) Betrachtet man aber nur Zahlen wie $a + b\sqrt{m}$, so kommt dies auf die Untersuchung eines Zahlrings im Körper $k(\sqrt{m_1})$ hinaus, und das setzt voraus, daß die Zahlkörper mit quadratfreier Grundzahl schon untersucht sind.

Dritter Abschnitt.

Anwendungen der Theorie des quadratischen Zahlkörpers.

34. Das „letzte Theorem" von Fermat.

Fermat hat in seiner Ausgabe des Diophant von Bachet (Oeuvres de Fermat, tome II, observations sur Diophante p. 291, II) den Satz aufgestellt, daß die Gleichung:

$$x^n + y^n = z^n,$$

für einen ganzzahligen positiven Exponenten $n > 2$ in ganzen rationalen Zahlen x, y, z nicht gelöst werden kann, wenn man von denjenigen Lösungen absieht, bei welchen eine der Unbekannten gleich Null gesetzt ist.

Fermat fügt hinzu, daß er diese Behauptung bewiesen habe. Außer dem Beweis, daß die Gleichung (s. Oeuvres t. I, p. 327, XXXIII und Beweis auf p. 340, XLV)

$$x^4 + y^4 = z^2$$

in dem angegebenen Sinn nicht lösbar sei, findet sich aber in seinen Werken keine Andeutung eines Beweises.

Erst Euler[1]) gelang es, den Beweis von Fermat auf den Fall $n = 3$ zu übertragen, und es haben später andere Mathematiker noch weitere spezielle Resultate gewonnen. So führten Legendre[2]) und Lejeune Dirichlet[3]) nach ganz verschiedenen Prinzipien den Unmöglichkeitsbeweis für $n = 5$, $n = 14$ und Lamé für $n = 7$.

---

1) Ziemlich eingehende historische Notizen über die verschiedenen Ansätze zum Beweis des Theorems findet man bei H. J. Smith, Collect. papers. Report II. p. 131. Die Beweise von Kummer hat Herr Hilbert in seinem Zahlber. Kap. XXXVI, S. 512 ff. sehr wesentlich vereinfacht. Ich habe mich hauptsächlich dieser Darstellung angeschlossen, die mir als die beste erscheint.

2) Legendre, Zahlentheorie, Bd. II, S. 1 u. 11 ff., ferner 348, und S. 352 ff. für $n = 5$.

3) Ges. Werke, Bd. I, S. 1, 21, 189 ff. Es handelt sich um die Fälle $n = 5$ und 14. Dirichlet gibt zugleich ganze Klassen von nicht lösbaren Gleichungen $x^5 + ay^5 = z^5$ usw. an.

Wieder andere Versuche, wie z. B. ein allgemeiner Beweis von Lamé[1]), waren von vornherein verfehlt, da sie den Satz von der eindeutigen Zerlegbarkeit algebraischer Zahlen involvierten; sie zeigten eben nur die Unzugänglichkeit des allgemeinen Problems. Erst Kummer[2]) ist es endlich gelungen, den Beweis im ganzen Umfange für alle Primzahlexponenten $n < 100$ zu führen. Außer den allgemeinen Reziprozitätsgesetzen ist es geradezu dieses Fermatsche Problem gewesen, welches Kummer zu seinen Untersuchungen und Entdeckungen betr. die komplexen Zahlen geleitet hat. Man zweifelt nicht mehr, daß die heutigen Hilfsmittel der Mathematik auch zur vollen Lösung des Problems ausreichen.

a) Entwicklungen von Fermat.

Es ist wohl durch das historische Interesse gerechtfertigt, wenn ich den Grundgedanken des Fermatschen und Eulerschen Beweises zunächst hier anführe.

Ich entwickle den Fermatschen Beweis für die Unlösbarkeit der Gleichung $x^4 + y^4 = z^2$ im wesentlichen nach der Darstellung von Legendre[3]), mit den Abkürzungen, welche die Lehre von den Zahlkörpern von selbst darbietet.

Bezüglich der Ausdrucksweise möge festgesetzt werden, daß der Satz: „die Gleichung $x^4 + y^4 = z^2$ ist unlösbar" besagen soll, daß es keine ganzzahligen rationalen Werte gibt, welche alle von Null verschieden sind und welche die Gleichung befriedigen.

Man kann ferner x, y, z als teilerfremd voraussetzen, da man einen ev. gemeinsamen Faktor durch Division wegschaffen könnte.

Wenn die Gleichung

$$x^4 + y^4 = z^2 \tag{1}$$

in ganzen, durchweg von Null verschiedenen Zahlen x, y, z lösbar ist, so bilden x^2, y^2, z eine Lösung der Diophantischen Gleichung:

$$(x^2)^2 + (y^2)^2 = z^2. \tag{1a}$$

Da nach dieser Darstellung z nur Primzahlen von der Form $4n + 1$ enthalten kann, abgesehen von solchen Faktoren, welche in x und y gleichzeitig enthalten sind, so kann z als Summe zweier

1) Comptes rendus. 1847. Vol. 24, p 310.

2) Verschiedene Abhandlungen aus dem Crelleschen Journal, Bd. 17, 40, sowie aus den Monatsber. der k. Akad. d. Wissensch., Berlin 1847, April, und Abhandl. der k. Akad. d. Wissensch., Berlin 1857.

3) Legendre, Zahlentheorie, übers. v. Maser 1886, Bd. II, S. 1 ff.

Quadrate dargestellt werden, und es muß daher jede Lösung folgendermaßen durch zwei ganze rationale Zahlen r, s ausdrückbar sein:

$$x^2 = r^2 - s^2, \quad y^2 = 2rs, \quad z = r^2 + s^2. \tag{3}$$

Setzt man von vornherein x, y, z teilerfremd voraus, so dürfen offenbar auch r und s keinen Teiler gemeinsam enthalten, es können ferner beide Größen positiv vorausgesetzt werden.

Betrachtet man nun die beiden Ausdrücke

$$x^2 = r^2 - s^2 \quad \text{und} \quad y^2 = 2rs,$$

so folgt zunächst aus der Voraussetzung, daß r und s keinen gemeinsamen Faktor haben und weil $y^2 = 2rs$, also y selbst gerade ist, daß entweder r und $2s$ oder auch $2r$ und s ganze rationale Quadratzahlen sind.

Ist etwa:

$$r = u^2$$
$$2s = 4v^2,$$

so wird

$$x^2 = u^4 - 4v^4. \tag{4}$$

Diese Gleichung ist nun wiederum eine Diophantische Gleichung, der genügt wird, wenn man die Substitution macht:

$$u^2 = a^2 + b^2 \tag{5}$$
$$v^2 = ab, \tag{6}$$

wo a und b teilerfremde ganze (positive) Zahlen sein sollen. Genau wie oben folgt aus (6) wieder, daß a und b Quadratzahlen sind.

Schreibt man daher:

$$a = f^2, \quad b = g^2,$$

so führt die Gleichung (5) auf die Gleichung:

$$u^2 = f^4 + g^4. \tag{7}$$

Diese Gleichung ist zwar der Form nach identisch mit der ursprünglichen Gleichung (1), aber nach der Konstruktion der Zahlen u, f, g ist jetzt:

$$\sqrt{r} = u \leqq \frac{y}{\sqrt{2}}, \quad s = \sqrt{2v^2} \leqq \frac{y}{\sqrt{2}},$$

denn es ist z. B. $s \geqq 1$, und:

$$r = \frac{y^2}{2s} \leqq \frac{y^2}{2},$$

also:

$$u \leqq \frac{y}{\sqrt{2}}, \quad v \leqq \frac{y}{2},$$

dann folgt aus (6) weiter:

$$a = f^2 \leqq \frac{y^2}{4}, \quad b = g^2 \leqq \frac{y^2}{4},$$

oder es ist:

$$f \leqq \frac{y}{2}, \quad g \leqq \frac{y}{2}.$$

Bezeichnen wir nun in der Gleichung (1) mit y den kleineren der beiden Werte x, y, so können wir das in der Gleichung (7) liegende Ergebnis so formulieren:

Ist die Gleichung (1) in ganzen (positiven) Zahlen lösbar, so kann man stets aus den Werten einer Lösung *kleinere* (positive) Werte konstruieren, welche ebenfalls eine Lösung der Diophantischen Gleichung (1) darstellen. Man kann dieses Verfahren fortsetzen und aus dem Zahlenpaar x, y unendlich viele andere positive Zahlenpaare f, g usw. ableiten, die immer kleiner werden und die Gleichung (1) befriedigen. Diesem Ergebnis widerspricht aber, daß unter einer positiven Zahl nur endlich viele andere positive kleinere Zahlen liegen. Die Annahme, daß Gleichung (1) eine Lösung besitzt, ist also unzulässig.

Ich schließe an den vorausgehenden Beweis noch einige Bemerkungen an:

1.) Durch den Beweis ist gezeigt; daß auch keine Gleichung von der Form

$$x^4 + y^4 = z^4$$

in ganzen Zahlen lösbar ist, ebensowenig ist die Gleichung:

$$x^8 + y^8 = z^2$$

lösbar, weil ja sonst die Lösung x^2, y^2, z die frühere Gleichung:

$$(x^2)^4 + (y^2)^4 = z^2$$

befriedigen würde. Allgemein ist die Gleichung unlösbar:

$$x^{2^n} + y^{2^n} = z^2.$$

2.) Von den Gleichungen (3) des vorstehenden Beweises können auch nicht zwei durch ganze rationale Zahlen x, y, z, r, s befriedigt werden. Setzt man daher statt $x^2 = r^2 - s^2$:

$$r + s = x_1^2$$
$$r - s = y_1^2,$$

was stets erlaubt ist, da x^2 ungerade sein soll und $r + s$, $r - s$ keinen gemeinsamen Faktor haben können, dann folgt:

$$2r = x_1^2 + y_1^2$$
$$2s = x_1^2 - y_1^2$$

und durch Ausmultiplizieren:

$$2y^2 = 4rs = x_1^4 - y_1^4.$$

Es ist also auch keine Gleichung von der Form

$$2z^2 = x^4 - y^4$$

lösbar.

3.) Da die Gleichung

$$x^4 + y^4 = z^4$$

in ganzen Zahlen nicht lösbar ist, so gibt es keine zwei Zahlen r und s, für die gleichzeitig

$$x^2 = r^2 - s^2$$

$$z^2 = r^2 + s^2$$

wäre. Die Gleichung:

$$x^2 z^2 = r^4 - s^4,$$

oder anders geschrieben:

$$z^2 = x^4 - y^4,$$

ist also ebenfalls unlösbar.

Fermat hat dieses letzte Resultat so formuliert: es gibt kein rechtwinkliges Dreieck mit ganzzahligen Seiten, dessen Inhalt gleich einer Quadratzahl ist.

Sind nämlich a, b die Katheten des Dreiecks, c die Hypotenuse, so müßten alsdann, wenn f auch eine ganze Zahl bezeichnet, die Gleichungen gelten:

$$xy = 2f^2$$

$$x^2 + y^2 = z^2,$$

oder:

$$(x - y)^2 = z^2 - 4f^2$$

$$(x + y)^2 = z^2 + 4f^2,$$

oder:

$$(x^2 - y^2)^2 = z^4 - (2f)^4;$$

dies sind aber Gleichungen, die nach den erhaltenen Resultaten in ganzen Zahlen x, y, z, f nicht lösbar sind.

Für den bisher entwickelten Fermatschen Beweis war ein Ansatz dadurch gewonnen, daß man von der Lösung der Diophantischen Gleichung

$$x^2 + y^2 = z^2$$

ausgehen konnte. Der *wesentliche* Grundgedanke des Beweises ist indes der, daß man aus der Annahme einer Lösung der Gleichung (1) unendlich viele andere Lösungen mit immer kleineren Werten der Unbekannten nachweisen kann.

Dieser selbe Grundgedanke läßt sich auch noch, wie Euler gezeigt hat, zum Beweis der Behauptung anwenden, daß die Gleichung

$$x^3 + y^3 = z^3$$

keine Lösung besitzt.

b) Entwicklung von Legendre.

Die Beweise, die Kummer für den „letzten Fermatschen Satz" gegeben hat, beruhen auf einem anderen Prinzip, das in seiner einfachsten Form Legendre[1]) schon verwendet hat und das wir an dem Beispiel der Gleichung: $x^3 + y^3 = z^3$, kurz auseinandersetzen wollen.

Satz. *Die Gleichung*

$$x^3 + y^3 = z^3 \tag{1}$$

ist unlösbar, d. h. sie kann nicht durch drei von Null verschiedene ganze rationale Zahlen für x, y, z befriedigt werden.

Beweis. Zunächst kann man voraussetzen, daß keine zwei der Zahlen x, y, z einen gemeinsamen Faktor besitzen, da derselbe sonst auch in der dritten Zahl stecken würde und sich folglich wegheben ließe. Wenn die Gleichung (1) lösbar ist, so darf man also von vornherein ausschließen, daß zwei der Zahlen x, y, z den Faktor 3 besitzen. Wenn man die Möglichkeit, daß eine der drei Zahlen durch 3 teilbar ist, für z allein zuläßt, so sind die Zahlen x, y modulo 3 so beschaffen, daß:

$$x \equiv \pm 1,\ (3) \quad \text{und} \quad y \equiv \pm 1,\ (3) \text{ ist.} \tag{2}$$

Bildet man nun die dritten Potenzen $(x \mp 1)^3$ und $(y \mp 1)^3$, so ergibt sich, daß:

$$x^3 \equiv \pm 1,\ (9), \quad y^3 \equiv \pm 1,\ (9) \tag{3}$$

ausfällt. Folglich sind für die Summe $x^3 + y^3$ zweier zu 3 primen Zahlen nur noch die nachstehenden Möglichkeiten vorhanden:

$$x^3 + y^3 \equiv \begin{cases} 2 \\ 0 \\ -2 \end{cases},\ (9). \tag{4}$$

Nimmt man zunächst an, daß auch z nicht durch 3 teilbar ist, so ist:

$$z^3 \equiv \pm 1,\ (9). \tag{5}$$

---

1) Zahlentheorie, Bd. II, S. 348 ff. Auch Gauß hat sich mit dem Beweis der Fermatschen Behauptung für komplexe Zahlen sogar beschäftigt, wie die aus dem Nachlaß herausgegebenen Notizen zeigen (vergl. Werke, Bd. II, S. 387 ff.), und zwar hat er zum Beweis für die Fälle $n = 3, 5$ ebenfalls das Prinzip der Beweise von Legendre und Kummer angewendet.

Alsdann ergibt aber die Zusammenfassung der Kongruenzen (4) und (5):

$$x^3 + y^3 - z^3 \equiv \begin{cases} \pm 1 \\ \pm 3 \end{cases}, (9),$$

so daß unmöglich die Gleichung $x^3 + y^3 - z^3 = 0$ oder

$$x^3 + y^3 = z^3$$

statthaben kann, weil dann der Ausdruck $x^3 + y^3 - z^3 \equiv 0, (9)$ wäre. Somit bleibt nur die Voraussetzung übrig, daß z durch 3 teilbar ist. Sei

$$z = 3^n z_1, \qquad (n \text{ eine ganze positive Zahl} \geqq 1),$$

dann ist also die Gleichung (1) nur lösbar, wenn sie von der Form ist:

$$x^3 + y^3 = 3^{3n} z^3. \tag{6}$$

Die Lösbarkeit dieser Gleichung (6) vorausgesetzt, muß

$$x \equiv \pm 1, (3), \quad \text{und gleichzeitig} \quad y \equiv \mp 1, (3)$$

sein. Man kann darum setzen:

$$x = p \pm q, \quad y = p \mp q, \tag{7}$$

wo p durch 3 teilbar ist, q aber nicht, und wo p und q teilerfremd, außerdem nicht gleichzeitig ungerade sind. Dann folgt:

$$x + y = 2p$$

$$x^2 - xy + y^2 = p^2 + 3q^2,$$

und die Gleichung (6) geht damit über in:

$$2p(p^2 + 3q^2) = 3^{3n} z^3. \tag{8}$$

Da die linke Seite dieser Gleichung gerade ist, so muß auch z eine gerade Zahl sein, dann wird aber:

$$z^3 = 2^{3m} z_1^{\,3}, \qquad (m \geqq 1)$$

und es muß ferner auch p gerade sein, weil $p^2 + 3q^2$ sicher ungerade ist.

Die beiden Faktoren

$$p \quad \text{und} \quad p^2 + 3q^2$$

haben wegen $p \equiv 0, (3)$ den gemeinsamen Faktor 3; andere Faktoren können dieselben aber nicht besitzen, da jeder Faktor zugleich in p und $3q^2$ enthalten sein muß.

Sind nun u, v zwei ganze teilerfremde Zahlen und: $u \cdot v = z_1$, so folgen daher aus (8) die beiden Gleichungen:

$$2p = 2^{3m} 3^{3n-1} u^3 \tag{9}$$

$$p^2 + 3q^2 = 3v^3. \tag{10}$$

Die linke Seite der Gleichung (10) ist im Körper $k(\sqrt{-3})$ die Norm einer ganzen Zahl, folglich ist auch v^3 und v selbst in diesem Körper zerlegbar, man kann daher die Relation ansetzen:

$$p + \sqrt{-3}\,q = \sqrt{-3}\,(f + \sqrt{-3}\,g)^3, \tag{11}$$

wo f und g wieder ganze teilerfremde Zahlen sind. Durch Ausmultiplizieren und Vergleichen beider Seiten erhält man aus Gleichung (11):

$$p = -9f^2g + 9g^3,$$

$$q = f^3 - 9fg^2,$$

also wird Gleichung (9):

$$2g(g-f)(g+f) = 2^{3m}3^{3n-3}u^3.$$

Diese Gleichung erfordert aber, da g, $g-f$ und $g+f$ keinen gemeinsamen Teiler besitzen können und da eine der beiden Zahlen g, f gerade, die andere ungerade sein muß, daß die rechte Seite zerfällt nach einem der zwei folgenden Systeme:

$$\begin{aligned} 2g &= 2^{3m}3^{3(n-1)}c^3 \quad &\text{oder}\quad 2g &= 2^{3m}c_1^3 \\ g-f &= b^3 & g-f &= 3^{3(n-1)}b_1^3 \\ g+f &= a^3 & g+f &= a_1^3. \end{aligned}$$

Hieraus folgt dann entweder:

$$a^3 + b^3 = 2^{3m}3^{3(n-1)}c^3, \quad \text{oder} \quad 2^{3m}c_1^3 = 3^{3(n-1)}b_1^3 + a_1^3.$$

Weil indessen im Fall der Lösbarkeit einer solchen Gleichung die durch 3 teilbare Zahl auch durch 2 teilbar sein muß, so könnte überhaupt nur die erste Gleichung bestehen, und es würde sich aus den angenommenen Lösungswerten auch eine Lösung der Gleichung:

$$x^3 + y^3 = 3^{3(n-1)}z^3$$

berechnen lassen. Durch Wiederholung käme man zu Werten, welche die Gleichung

$$x_1^3 + y_1^3 = z_1^3$$

befriedigen, wo nun x_1, y_1 und z_1 nicht durch 3 teilbar sind. Dies widerspricht aber der zuerst gemachten Bemerkung, daß z_1 durch 3 teilbar sein müßte. Die Gleichung

$$x^3 + y^3 = z^3$$

kann also in der Tat keine Lösung besitzen.

Weitere Bemerkungen, die sich an dieses Ergebnis anschließen, sollen später folgen. Zunächst behandle ich nun die beiden Sätze auf Grund der Lehre von den Zahlkörpern.

e) Entwicklungen von Kummer und Hilbert.

Kummer hat das Fermatsche Problem noch erheblich erweitert, indem er zeigte, daß die Gleichung:

$$x^n + y^n = z^n,$$

für $n > 2$ nicht bloß in ganzen rationalen Zahlen, sondern auch in den ganzen Zahlen des durch die $\sqrt[n]{1}$ bestimmten Zahlkörpers unlösbar ist.

Für den Fall $n = 3$ lautet Kummers Behauptung folgendermaßen:

Satz. *Die Gleichung*

$$\alpha^3 - \beta^3 = \gamma^3 \tag{1}$$

ist nicht lösbar in ganzen Zahlen des Körpers $k(\sqrt{-3})$. Oder, wenn α, β, γ drei ganze von Null verschiedene Zahlen des Körpers $k(\sqrt{-3})$ bezeichnen, so kann zwischen denselben keine Relation von der Form:

$$\alpha^3 - \beta^3 = \gamma^3 \tag{1}$$

bestehen.

Beweis. Die Klassenanzahl des Körpers $k(\sqrt{-3})$ ist $h = 1$, und es sei, mit einer kleinen Änderung der Bezeichnung, gegen früher, $\omega = \frac{-1-\sqrt{-3}}{2}$. Falls die Gleichung (1) überhaupt lösbar ist, so kann man irgend zwei der Zahlen α, β, γ als teilerfremd voraussetzen. Bedeuten aber α, β, γ drei teilerfremde Zahlen des Körpers $k(\sqrt{-3})$ und setzt man:

$$\lambda = 1 - \omega,$$

also

$$(\lambda) = (\sqrt{-3}),$$

so läßt sich zunächst zeigen: wenn die Gleichung (1) in ganzen Zahlen des Körpers $k(\sqrt{-3})$ lösbar ist, so muß eine der 3 Zahlen α, β, γ den Faktor λ enthalten.

Sind nämlich α, β nicht durch λ teilbar, und schreibt man etwa:

$$\alpha = a + b\omega = (a + b) - b(1 - \omega),$$

so ist $a + b$ sicher nicht durch λ und umsoweniger durch 3 teilbar. Da dann stets:

$$a + b \equiv \pm 1,\ (3)$$

sein muß, so ist notwendig:

$$\alpha \equiv \pm 1,\ (\lambda),$$

desgleichen:

$$\beta \equiv \pm 1,\ (\lambda).$$

Wie man leicht erkennt, ergibt sich hieraus, daß für die Differenz $\alpha^3 - \beta^3$ in bezug auf λ^3 eine der drei folgenden Kongruenzen statthaben muß:

$$\alpha^3 - \beta^3 \equiv \begin{cases} -2 \\ 0, \\ +2 \end{cases} (\lambda^3).$$

Wenn auch die dritte Zahl γ prim zu λ vorausgesetzt ist, also:

$$\gamma \equiv \pm 1, \ (\lambda)$$

angenommen wird, so ergeben sich für den Ausdruck $\alpha^3 - \beta^3 - \gamma^3$ modulo λ^3 folgende Möglichkeiten:

$$\alpha^3 - \beta^3 - \gamma^3 \equiv \begin{cases} \pm 3 \\ \pm 1, \end{cases} (\lambda^3).$$

Weil indessen:

$$\pm 3 \not\equiv 0, \quad \pm 1 \not\equiv 0, \ (\lambda^3)$$

ist, kann umsoweniger

$$\alpha^3 - \beta^3 - \gamma^3 = 0,$$

oder

$$\alpha^3 - \beta^3 = \gamma^3$$

sein. D. h., wenn die Gleichung (1) lösbar ist, dann muß jedenfalls eine der drei Zahlen α, β, γ durch λ teilbar sein.

Es sei nun γ die durch λ teilbare Zahl, mithin

$$\gamma = \lambda^n \gamma_1, \qquad n \geqq 1,$$

so läßt sich jetzt durch eine genauere Untersuchung der Zahlen α und β weiter zeigen, daß der Exponent $n \geqq 2$ sein muß. Indem man nämlich die zu λ prime Zahl $\alpha = a + b\omega$ betrachtet, ist:

entweder

$$a \equiv \pm 1, \ (3), \qquad b \equiv 0, \ (3),$$

dann kann man aber:

$$\alpha = \pm 1 + \lambda^2 \alpha_1,$$

setzen, wo α_1 eine ganze Zahl des Körpers ist;

oder

$$a \equiv \pm 1, \ (3) \quad \text{und gleichzeitig} \quad b \equiv \pm 1, \ (3),$$

weil

$$a + b \equiv \pm 1, \ (3)$$

sein muß; dann wird:

$$\alpha = a + b\omega = \pm (1 + \omega) + \lambda^2 \alpha_1,$$

wo jetzt:

$$\eta = 1 + \omega$$

eine Einheit des Körpers ist.

Bezeichnet man mit η, η_1 usw. Einheiten des Körpers, so gilt daher für die zu λ prime Zahl α eine Kongruenz:

$$\alpha \equiv \eta, \ (\lambda^2),$$

und analog für β:

$$\beta \equiv \eta_1, \ (\lambda^2).$$

Wegen der Kongruenz:

$$\alpha^3 - \beta^3 \equiv 0, \ (\lambda^3)$$

muß dann

$$\eta^3 - \eta_1{}^3 = 0$$

sein, folglich ist:

$$\alpha^3 - \beta^3 \equiv 0, \ (\lambda^4).$$

Soll also die Gleichung (1) bestehen, so muß γ mindestens durch λ^2 teilbar sein, d. h. in der Gleichung $\gamma = \lambda^n \gamma_1$ ist $n \geqq 2$ zu nehmen.

Nun läßt sich die Unlösbarkeit der Gleichung (1) zeigen, indem man beweist, daß auch die noch etwas allgemeinere Gleichung:

$$\alpha^3 - \beta^3 = \eta \lambda^{3n} \gamma^3, \tag{2}$$

wobei η eine Einheit des Körpers bezeichnet, nicht lösbar sein kann.

Wegen der Bedingungen:

$$\alpha \equiv \pm 1, \ (\lambda), \quad \beta \equiv \pm 1, \ (\lambda),$$
$$\alpha^3 - \beta^3 \equiv 0, \ (\lambda^3)$$

müssen α, β die simultanen Bedingungen erfüllen:

$$\alpha \equiv \pm 1, \ (\lambda), \quad \beta \equiv \pm 1, \ (\lambda),$$

woraus dann die simultanen Kongruenzen folgen:

$$\left.\begin{aligned} \alpha - \beta \ &\equiv 0 \\ \alpha - \omega\beta \ &\equiv 0 \\ \alpha - \omega^2\beta &\equiv 0 \end{aligned}\right\}, \ (\lambda).$$

Von den drei Differenzen $\alpha - \beta$, $\alpha - \omega\beta$, $\alpha - \omega^2\beta$ kann nur eine die Zahl λ zu einer höheren als zur ersten Potenz enthalten. Wenn man nun annimmt, es sei $\alpha - \beta$ mindestens durch λ^2 teilbar, so können $\alpha - \omega\beta$ und $\alpha - \omega^2\beta$ nur durch λ teilbar sein, denn es ist z. B.

$$\frac{\alpha - \omega\beta}{\lambda} \equiv \pm 1, \ (\lambda),$$

da ferner α und β prim zueinander sind, so können die drei Zahlen $\alpha - \beta$, $\alpha - \omega\beta$, $\alpha - \omega^2\beta$ überhaupt keinen weiteren Faktor außer λ gemeinsam haben, woraus dann schließlich folgt, daß der Relation (2) oder:

$$(\alpha - \beta)(\alpha - \omega\beta)(\alpha - \omega^2\beta) = \eta \lambda^{3n} \gamma^3 \tag{2a}$$

nur so zu genügen ist, daß man setzt:

$$\left.\begin{aligned} \alpha - \beta \quad &= \eta_1 \lambda^{3n-2} \tau^3 \\ \alpha - \omega\beta \ &= \eta_2 \lambda \mu^3 \\ \alpha - \omega^2\beta &= \eta_3 \lambda \nu^3, \end{aligned}\right\} \tag{3}$$

wo η_1, η_2, η_3 Einheiten des Körpers und τ, μ, ν ganze teilerfremde Zahlen bezeichnen. Wegen der Gleichung:

$$\omega(\alpha - \beta) + \omega^2(\alpha - \omega\beta) + (\alpha - \omega^2\beta) = 0,$$

ergibt sich dann aus dem Gleichungssystem (3):

$$\omega\eta_1\lambda^{3n-2}\tau^3 + \eta_2\omega^2\lambda\mu^3 + \eta_3\lambda\nu^3 = 0,$$

oder wenn mit $\omega^2\eta_2\lambda$ dividiert wird und für die noch bleibenden Einheiten die Buchstaben ζ resp. ζ_1 geschrieben werden:

$$\mu^3 - \zeta\nu^3 = \zeta_1\lambda^{3(n-1)}\tau^3.$$

Um die Einheit ζ zu bestimmen, faßt man die letzte Gleichung als Kongruenz nach λ^3 auf, was wegen $n \geqq 2$ erlaubt ist. Dann ist:

$$\mu^3 - \zeta\nu^3 \equiv 0, \ (\lambda^3).$$

Nun sind μ, $\nu \equiv \pm 1$, (λ) und μ^3, $\nu^3 \equiv \pm 1$, (λ^3); daher kann die letzte Gleichung offenbar nur erfüllt sein, wenn:

$$\zeta \equiv \pm 1, \ (\lambda^3),$$

d. h. wenn

$$\zeta = \pm 1$$

ist.

Man ist also durch die Voraussetzung der Lösbarkeit der Gleichung (2) darauf geführt, daß auch

$$\alpha^3 - \beta^3 = \zeta_1\lambda^{3(n-1)}\gamma^3$$

eine Lösung besitzt. Durch die wiederholte Anwendung des Verfahrens auf die letzte Gleichung und die Fortsetzung des Prozesses gelangt man dann zu einer Gleichung:

$$\alpha^3 - \beta^3 = \eta\lambda^3\gamma^3,$$

wo nun alle drei Zahlen α, β, γ den Faktor λ nicht mehr enthalten. Das Bestehen dieser letzten Gleichung widerspricht den Anforderungen, denen eine Lösung genügen müßte. Die Voraussetzung des Beweises ist also unzulässig. Die Gleichung (2) und umsomehr auch die Gleichung (1) ist in ganzen Zahlen des Körpers $k(\sqrt{-3})$ nicht lösbar.

Zum Schlusse soll noch die Kummersche Verallgemeinerung des Fermatschen Satzes für $n = 4$ bewiesen werden.

Satz. *Die Diophantische Gleichung*

$$\alpha^4 + \beta^4 = \gamma^2$$

ist in ganzen Zahlen des Körpers $k(\sqrt{-1})$ *nicht lösbar, wenn alle drei Zahlen* α, β, γ *von Null verschieden sein sollen.*

Beweis. Anstelle der gegebenen Gleichung sei zugrunde gelegt:

$$\alpha^4 = \gamma^2 - \beta^4. \tag{1}$$

α, β, γ seien ohne gemeinsamen Faktor. Wenn nun:

$$\lambda = 1 - \sqrt{-1}$$

gesetzt wird, so läßt sich zunächst zeigen, daß im Falle der Lösbarkeit der Gleichung (1) eine der Zahlen α oder β notwendig den Faktor λ enthalten muß, während die übrigen beiden Zahlen diesen Faktor λ nicht besitzen.

Bekanntlich sind die Zahlen 2, $\pm(1 \pm \sqrt{-1})$ durch λ teilbar, denn es ist ja $2 = n(\lambda)$ und $\lambda' = \sqrt{-1}\,\lambda$. Jede ganze Zahl α des Körpers, welche zu λ prim ist, genügt einer Kongruenz:

$$\alpha \equiv \sqrt{-1},\ (\lambda);$$

ferner genügt jede ganze Zahl, welche relativ prim zu 2 ist, einer der beiden Kongruenzen:

$$\alpha \equiv \sqrt{-1},\ (2) \quad \text{oder} \quad \alpha \equiv 1,\ (2), \tag{2}$$

denn es gibt nur zwei zu 2 relativ prime Restzahlen.

Aus jeder dieser Kongruenzen (2) folgt sodann weiter:

$$\alpha^4 - 1 \equiv 0,\ (\lambda^6),$$

d. h. die vierte Potenz jeder zu λ relativ primen ganzen Zahl des Körpers ist stets kongruent $+1$ nach dem Modul λ^6 oder nach 8.

Nimmt man jetzt zuerst an, die Gleichung (1) bestehe für ganze Zahlen α, β, γ, von denen α, β prim sind zu λ. Dann ist:

$$\alpha^4 \equiv 1,\ (\lambda^6) \quad \text{und} \quad \beta^4 \equiv 1,\ (\lambda^6), \tag{3}$$

folglich:

$$\alpha^4 + \beta^4 - 2 \equiv 0,\ (\lambda^6).$$

Aus der Gleichung

$$\alpha^4 + \beta^4 - 2 = \gamma^2 - 2 \tag{4}$$

folgt nun weiter, daß γ durch λ^1 teilbar, oder daß $\gamma = \lambda\gamma_1$ sein müßte, wo nun γ_1 prim ist zu λ. Alsdann wird aber

$$\gamma^2 - 2 = \lambda^2\gamma_1^2 - 2 = -2\sqrt{-1}\,(\gamma_1^2 - \sqrt{-1}),$$

d. h. es müßte die Kongruenz bestehen:

$$\gamma_1^2 - \sqrt{-1} \equiv 0,\ (\lambda^4);$$

dies ist nicht der Fall, weil für irgend eine ganze Zahl γ_1 nur eine der beiden Kongruenzen $\gamma_1^2 \equiv +1$, oder $\gamma_1^2 \equiv -1$, (λ^4) möglich ist.

Nimmt man zweitens an, die Zahlen β und γ seien prim zu λ, so ist stets

$$\gamma^2 \equiv 1,\ (\lambda^2) \quad \text{und} \quad \beta^4 \equiv 1,\ (\lambda^2),$$

die Differenz $\gamma^2 - \beta^4$ ist also mindestens durch λ^2 teilbar; d. h. es muß notwendig $\alpha \equiv 0$, (λ) oder $\alpha = \lambda^n \alpha_1 (n \geqq 1)$ sein, wenn die Gleichung (1) für ganze Zahlen des Körpers $k(\sqrt{-1})$ zu Recht besteht.

Die Gleichung (1) ist also *nur* lösbar, wenn die Gleichung $\lambda^{4n}\alpha^4 = \gamma^2 - \beta^4$ lösbar ist, und umgekehrt.

Man ersetzt nun die letztere Gleichung wieder durch eine etwas noch allgemeinere Gleichung:

$$\varepsilon \lambda^{4n} \alpha^4 = \gamma^2 - \beta^4, \tag{5}$$

in der ε eine Einheit von $k(\sqrt{-1})$ bezeichnet und untersucht die Lösbarkeit dieser Gleichung.

Die Gleichung (5) kann etwas anders geschrieben werden:

$$\gamma^2 - 1 = \varepsilon \lambda^{4n} \alpha^4 + \beta^4 - 1;$$

da $\beta^4 - 1$ stets durch λ^6 teilbar ist, so folgt, daß $\gamma^2 - 1$ mindestens durch λ^4 teilbar sein muß, wenn die Gleichung (5) lösbar sein soll, oder es ist:

$$\gamma^2 \equiv 1,\ (\lambda^4). \tag{6}$$

Diese Kongruenz kann aber nur erfüllt sein, wenn von den beiden Möglichkeiten $\gamma \equiv \sqrt{-1}$ oder $\gamma \equiv 1$, (λ^2) die zweite vorliegt. Setzt man dann etwa:

$$\gamma - 1 = \lambda^2 \tau, \quad \text{so wird:} \quad \gamma + 1 = \lambda^2(\tau + \sqrt{-1}),$$

und da $\tau + \sqrt{-1}$ durch λ teilbar ist, so gilt daher die Kongruenz:

$$\gamma^2 - 1 \equiv 0,\ (\lambda^5).$$

Somit ist die rechte Seite der Gleichung (5) jedenfalls durch λ^5 teilbar, und das bedingt, daß der Exponent $n \geqq 2$ vorausgesetzt werden muß.

Schreibt man jetzt die Gleichung (5) in der Form:

$$\varepsilon \lambda^{4n} \alpha^4 = (\gamma - \beta^2)(\gamma + \beta^2), \tag{7}$$

und bemerkt, daß $\gamma - \beta^2$ und $\gamma + \beta^2$ außer λ^2 keinen gemeinsamen Teiler besitzen können, da jeder solche Teiler zugleich in 2γ und $2\beta^2$ aufgehen muß, so kann man die Gleichung (7) z. B. durch das nachfolgende System ersetzen:

$$\left.\begin{aligned} \gamma - \beta^2 &= \eta \lambda^2 \sigma^4 \\ \gamma + \beta^2 &= \eta_1 \lambda^{4n-2} \tau^4, \end{aligned}\right\} \qquad (8)$$

in dem σ, τ zwei ganze teilerfremde Zahlen, η, η_1 Einheiten des Körpers $k(\sqrt{-1})$ bezeichnen. Durch Subtraktion der Gleichungen (8) folgt:

$$2\beta^2 = \eta_1 \lambda^{4n-2} \tau^4 - \eta \lambda^2 \sigma^4,$$

oder wenn diese Gleichung mit 2 dividiert wird, und anstelle von $-\frac{\eta \lambda^2}{2}$ und $\frac{\eta_1 \lambda^2}{2}$ die Einheiten ζ und ζ_1 geschrieben werden:

$$\beta^2 - \zeta \sigma^4 = \zeta_1 \lambda^{4(n-1)} \tau^4. \qquad (9)$$

Da $n \geqq 2$ ist, folgt aus dieser Gleichung zur Bestimmung von ζ eine Kongruenz nach dem Modul λ^4:

$$\beta^2 - \zeta \sigma^4 \equiv 0, \ (\lambda^4) \quad \text{oder} \quad \beta^2 - \zeta \equiv 0, \ (\lambda^4),$$

und aus dieser ergibt sich $\zeta = \pm 1$. D. h. wenn die Gleichung (5) lösbar ist, so ist auch die Gleichung (9) oder anders geschrieben:

$$\varepsilon \lambda^{4(n-1)} \alpha^4 = \gamma^2 - \beta^4 \qquad (10)$$

lösbar. Wendet man nun dieselbe Schlußweise, die eben zur Untersuchung der Gleichung (5) gedient hat, auf die Gleichung (10) an und wiederholt das Verfahren, so gelangt man schließlich zu der Folgerung, daß auch die Gleichung:

$$\varepsilon \lambda^4 \alpha^4 = \gamma^2 - \beta^4,$$

lösbar ist, was nach den ersten Erörterungen über die ev. Lösungswerte der Gleichung (1) oder (5), worin $n \geqq 2$ sein muß, nicht zutrifft. Die Annahme des Beweises ist also falsch, und folglich gilt die Behauptung des Satzes.

Aus diesem Beweis der Fermatschen Behauptung folgt unmittelbar, daß weder die Gleichung:

$$z^2 = x^4 + y^4,$$

noch die Gleichung:

$$z^2 = x^4 - y^4$$

durch ganze rationale Zahlen, welche sämtlich von Null verschieden sind, lösbar sein kann.

Endlich ist es nur eine andere Form der Fermatschen Behauptung, wenn man sagt, daß die Gleichungen:

$$x^3 + y^3 = z^3$$

und

$$x^4 \pm y^4 = z^2,$$

auch nicht für irgend welche gebrochenen rationalen Zahlen bestehen können, die alle drei von Null verschieden sind.

Eine Konsequenz der Beweise ist ferner, daß überhaupt keine Gleichung:

$$x^{3n} \pm y^{3n} = z^{3n}$$

oder

$$x^{4n} \pm y^{4n} = z^2 \qquad n > 1$$

in ganzen Zahlen, von denen keine gleich Null ist, bestehen kann, denn jede Lösung ergäbe notwendig eine Lösung der Gleichung

$$x^3 \pm y^3 = z^3$$

resp.

$$x^4 \pm y^4 = z^2.$$

In etwas veränderter Fassung lautet das Fermatsche Theorem in den von uns behandelten Fällen so: für irgend welche rationalen Zahlen x sind

$$\sqrt[3]{1 \pm x^3}, \quad \sqrt[4]{1 \pm x^4}$$

stets irrational.

In geometrischer Form würde das Fermatsche Theorem aussagen, daß diejenigen Kurven

$$x^3 \pm y^3 = c^3$$

$$x^4 \pm y^4 = c^2,$$

für welche c eine rationale Zahl ist, niemals durch Punkte mit rationalen Koordinaten hindurchgehen können.

Für den Fall $l = 3$ kann man aber noch weiter gehen. Es ist leicht einzusehen, daß die Gleichungen

$$x^3 \pm y^3 = z^3$$

auch nicht für Quadratwurzeln aus irgend welchen ganzen rationalen Zahlen bestehen können. Sind nämlich a, b, c drei teilerfremde Zahlen, die nicht Quadratzahlen sind, so folgt aus:

$$\sqrt{a^3} \pm \sqrt{b^3} = \sqrt{c^3},$$

die Gleichung:

$$a^3 + b^3 - c^3 = \mp 2\sqrt{a^3 b^3};$$

da nun links eine ganze rationale Zahl steht, so müßte

$$\sqrt{a^3 b^3}$$

ebenfalls rational sein, was nicht möglich ist, da nach der Voraussetzung a, b weder Quadratzahlen sind, noch einen gemeinsamen Faktor enthalten.

Es liegen also auf einer Kurve

$$x^3 \pm y^3 = c^3$$

mit der rationalen Konstanten c auch keine Punkte, deren Koordinaten durch Quadratwurzeln aus rationalen Zahlen sich ausdrücken.

Für spätere Untersuchungen über die Zahlkörper vom dritten Grade ist eine Folgerung sehr nützlich, welche Kronecker[1]) aus der Tatsache gezogen hat, daß die Gleichung

$$x^3 + y^3 = 1$$

in rationalen Zahlen nur lösbar ist, wenn x oder y Null gesetzt wird.

Vorausgesetzt, daß die Gleichung $x^3 + y^3 = 1$ irgend welche rationale Lösungen besitzt, so könnte man das Lösungssystem x, y durch zwei andere rationale Zahlen a, b in der Gestalt:

$$x = \frac{2a}{3b-1}, \quad y = \frac{3b+1}{3b-1}$$

darstellen. Mit diesen Formeln wird nun:

$$x^3 + y^3 - 1 = \frac{2\{4a^3 + 27b^2 + 1\}}{(3b-1)^3},$$

und jede rationale Lösung der Gleichung $x^3 + y^3 - 1 = 0$ ergibt gleichzeitig eine rationale Lösung der Gleichung:

$$4a^3 + 27b^2 + 1 = 0.$$

Weil aber die Gleichung $x^3 + y^3 - 1 = 0$ nur die Lösungen $x = 1$, $y = 0$ (oder $x = 0$, $y = 1$) besitzt, so kann die Gleichung:

$$4a^3 + 27b^2 + 1 = 0,$$

nur die Zahlen $a = -1$, $b = \pm\frac{1}{3}$ als einzige rationale Lösungen besitzen.

Beachtet man jetzt[2]), daß:

$$\Delta = -(4a^3 + 27b^2),$$

die Diskriminante der Gleichung dritten Grades:

$$x^3 + ax + b = 0$$

ist, oder das Quadrat des Produktes der Wurzeldifferenzen dieser Gleichung:

$$(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2,$$

darstellt, so lautet das Ergebnis der Untersuchung folgendermaßen:

1) L. Kronecker, Werke, I. Bd. 1895, S. 121 oder Crelles Journal, Bd. 56, S. 188.

2) Vergl. z. B. H. Weber, Lehrbuch der Algebra. 2. Aufl. 1898. Bd. I, S. 168.

Satz. *Die Gleichungen:*

$$x^3 - x \pm \tfrac{1}{3} = 0,$$

sind die beiden einzigen Gleichungen dritten Grades mit rationalen Koeffizienten, für welche das Produkt der drei quadrierten Wurzeldifferenzen $+1$ *wird, während zugleich die Summe der drei Wurzeln den Wert Null hat.*

Die weiteren Fälle der Gleichung $x^n + y^n = z^n$, wo $n \geqq 5$ angenommen ist, erfordern zu ihrer Behandlung Hilfsmittel aus der Lehre von den allgemeinen algebraischen Zahlen, die in diesem Buche nicht entwickelt sind. Wir müssen daher die Untersuchung der Fermatschen Behauptung hier abbrechen und wenden uns nun zu einer weiteren *Anwendung der Lehre vom quadratischen Zahlkörper auf die Eigenschaften der quadratischen Formen.*

35. Überblick über die Fundamentalprobleme der Theorie der quadratischen Formen.

Bei der Untersuchung spezieller Zahlkörper, so z. B. der Körper $k(\sqrt{-1})$, $k(\sqrt{2})$ usw. haben sich Bedingungen ergeben zur Entscheidung darüber, wann eine rationale Zahl a durch einen Ausdruck

$$x^2 + y^2, \quad \text{oder} \quad x^2 - 2y^2, \quad \text{oder} \quad x^2 + 3y^2$$

usw. usw. darstellbar ist, oder anders ausgedrückt, wann eine Diophantische Gleichung von der Form:

$$a = x^2 - my^2,$$

durch ganze rationale Zahlen x, y befriedigt werden kann.

Diese Sätze sind Spezialfälle einer allgemeinen Theorie, nämlich der Theorie der quadratischen Formen.

Man nennt jeden Ausdruck:

$$f = ax^2 + 2bxy + cy^2,$$

in welchem a, b, c gegebene Zahlen, x, y Veränderliche sind, eine homogene *quadratische Form*, und es wird insbesondere in der Zahlentheorie stets vorausgesetzt, daß die Koeffizienten a, $2b$, c *ganze* rationale Zahlen sind.

a, b, c heißen die Koeffizienten der Form, und zwar a, c die äußeren Koeffizienten, b der mittlere Koeffizient. Gauß hat in seinen Untersuchungen stets $2b$ als *gerade* vorausgesetzt.

Nachdem schon Euler durch die Untersuchung besonderer quadratischer Formen zu sehr bemerkenswerten Entdeckungen geführt worden

war, griff zuerst Lagrange die Untersuchung der allgemeinen quadratischen Formen vom Gesichtspunkt der Zahlentheorie aus an und entwickelte dazu die Eigenschaften der Kettenbrüche. Legendre hat diese Untersuchungen weitergeführt und seine Ergebnisse in Verbindung mit den Untersuchungen der älteren Mathematiker in seiner „théorie des nombres“ dargestellt.

Den größten Fortschritt in der Theorie der quadratischen Formen verdankt man aber Gauß[1]). Fast die gesamte sectio V der Disquis. arithmet., nahezu die Hälfte des ganzen Werkes, ist diesem Gegenstande gewidmet.

Die Darstellung von Gauß ist nach Form und Inhalt für die Zahlentheorie vorbildlich geworden, ja es rühren die fruchtbarsten Methoden und reiche und tiefliegende Probleme von Gauß selbst her.

Ich will hier zunächst eine Reihe wichtiger, notwendiger Bezeichnungen erklären und dann die fundamentalen Fragestellungen aus der Theorie der quadratischen Formen anführen, um schließlich den Zusammenhang mit der Körpertheorie darzustellen.

Nach Gauß heißt eine quadratische Form:

$$F = ax^2 + 2bxy + cy^2,$$

eigentlich *primitiv*, wenn a, $2b$, c keinen gemeinsamen Faktor besitzen, und *uneigentlich primitiv*, falls a, $2b$, c die Zahl 2 als größten gemeinsamen Faktor besitzen. Die Diskriminante:

$$D = b^2 - ac,$$

heißt die *Determinante* der quadratischen Form. Die Determinante kann positiv oder negativ sein, was wesentliche Unterschiede für die Behandlung der entsprechenden Formen bedingt, ähnlich wie dies ja auch für reelle und imaginäre Körper der Fall ist.

Der wichtigste Fall der quadratischen Formen, auf den wir uns beschränken, ist derjenige, daß D keine quadratischen Faktoren enthält. Der Fall, daß $D = 0$ ist, wird im folgenden ganz ausgeschlossen.

Führt man in einer Form F mit der Determinante D an Stelle von x und y neue Veränderliche x_1, y_1 ein, durch eine Substitution mit ganzen rationalen Koeffizienten:

$$x = rx_1 + sy_1,$$
$$y = tx_1 + uy_1,$$

1) Zum Verständnis dieser Nummer vergleiche der Leser außer den oben genannten Werken von Gauß und Legendre die entsprechenden Kapitel in den Lehrbüchern von Dirichlet-Dedekind, oder Bachmann usw.

so erhält man eine neue Form:

$$f = Ax_1^2 + 2Bx_1y_1 + Cy_1^2,$$

oder wenn zur Abkürzung der Index 1 an den Veränderlichen weggelassen wird:

$$f = Ax^2 + 2Bxy + Cy^2.$$

Die Determinante der Form f, von der man sagt, daß sie durch Transformation aus der Form F *abgeleitet* sei, ist:

$$D_1 = \begin{vmatrix} r & s \\ t & u \end{vmatrix}^2 \cdot D = \Delta^2 \cdot D,$$

wo Δ die Transformationsdeterminante heißt.

Wenn Δ von ± 1 verschieden ist, so sagt man, die Form f *sei unter der Form F enthalten,* wenn dagegen $\Delta = \pm 1$ ist, so bezeichnet man die Formen F und f als *äquivalent,* und zwar heißen die beiden Formen *eigentlich äquivalent,* wenn $\Delta = +1$ ist, und *uneigentlich äquivalent,* wenn $\Delta = -1$ ist. In beiden Fällen ist, wie man sofort sieht, die Form f unter der Form F, aber auch umgekehrt die Form F unter der Form f enthalten.

Indem man r, s, t, u so wählt, daß

$$\Delta = ru - st = +1$$

ist, kann man aus einer Form unendlich viele andere ihr eigentlich äquivalente Formen ableiten.

Berücksichtigt man, daß sich zwei Transformationen zu einer einzigen zusammenfassen lassen, deren Determinante alsdann gleich dem Produkt der Determinanten der einzelnen Transformationen ist, so kann man leicht einsehen, daß zwei Formen untereinander äquivalent sind, wenn sie beide einer dritten Form äquivalent sind. Man erhält daher die sämtlichen äquivalenten Formen, wenn man von irgend einer dieser Formen ausgeht. Es ist damit die Möglichkeit gegeben, alle untereinander äquivalenten Formen zu einem Inbegriff zusammenzufassen.

Alle untereinander äquivalenten Formen bilden zusammen eine *Klasse.* Man kann beweisen, daß alle überhaupt möglichen Formen mit derselben Determinante D sich auf eine *endliche* Anzahl von Klassen verteilen.

Die fundamentalen Probleme der Theorie der quadratischen Formen sind nun die folgenden:

1.) Zu entscheiden, ob eine gegebene Zahl durch eine gegebene Form darstellbar ist, und die Werte der Veränderlichen x, y anzugeben, welche diese Darstellung leisten.

2.) Zu entscheiden, ob zwei gegebene quadratische Formen mit derselben Determinante D äquivalent sind, und die Transformationsformeln aufzustellen, welche ev. die beiden Formen ineinander überführen.

3.) Zu beweisen, daß die unendlich vielen Formen sich auf eine endliche Anzahl von Klassen verteilen.

4.) Für die einzelnen Klassen repräsentierende Formen zu definieren, um die erste Aufgabe auf die Ausführung weniger Rechnungen zu beschränken.

Gerade das erste Problem hat den Anstoß gegeben zu allen Untersuchungen über die quadratischen Formen, es ist gewissermaßen „das" Problem derselben.

Wenn eine Zahl durch eine quadratische Form F darstellbar ist, so ist sie auch durch jede andere Form F_1 darstellbar, welche zu F äquivalent ist. Die Lösung der ersten Aufgabe wird daher dadurch erleichtert, daß man zunächst einfache Formen aufsucht, durch welche die Darstellung der gegebenen Zahl möglichst bequem geleistet wird.

Eine weitere Aufgabe der Theorie der quadratischen Formen ist schließlich die Einteilung der Klassen in Geschlechter.

Zu der Zeit (1801), als Gauß seine Untersuchungen über die höhere Arithmetik veröffentlichte, hatten die imaginären Größen nicht die volle Gleichberechtigung mit den reellen. Wegen scheinbarer innerer Widersprüche, die der Begriff der imaginären Größen enthalten sollte, und wegen mancher falscher Verwendungen waren dieselben in Mißkredit gekommen.

Wenn auch Gauß dieses Vorurteil seiner Zeit gewiß nicht teilte, so umging er in seinen Abhandlungen doch noch den Gebrauch des Imaginären, und er hat so die Theorie der quadratischen Formen rein auf die Eigenschaften der reellen rationalen Zahlen aufgebaut.

Indessen hat Kummer[1]) gleich in seinen ersten Mitteilungen über die Entdeckung der Ideale darauf hingewiesen, daß die Theorien des quadratischen Zahlkörpers und der quadratischen Formen identisch sind. Die Verwendung der quadratischen, reellen und imaginären Zahlen dient sogar zu einer wesentlichen Vereinfachung der Formentheorie. (Vergl. insbesondere Dedekind, Vorlesungen über Zahlentheorie von Lejeune-Dirichlet, § 71 ff. und Suppl. XI, § 186 ff.)

Ich will den Zusammenhang zwischen Zahlkörper und quadratischen Formen hier im einzelnen genauer verfolgen. Es ist dazu eigentlich nur

---

1) Crelles Journal, Bd. 35, p. 325.

notwendig, eine genaue Zuordnung von Ideal und quadratischer Form zu treffen, dann ergibt sich von selbst die Übertragung der Multiplikation der Ideale, des Begriffs der Idealklasse und des Geschlechtes auf die quadratischen Formen.

Die Zuordnung von Idealen und Formen ist für reelle Körper etwas komplizierter als für imaginäre Körper. Es soll daher hauptsächlich der Fall reeller Körper behandelt werden.

36. Zuordnung der Ideale und quadratischen Formen.
(Darstellung von Zahlen durch quadratische Formen.)

Es bezeichne $\mathfrak{p} = (p,\, b + \sqrt{m})$ irgend ein Primideal des Körpers $k(\sqrt{m})$, dann sind alle Zahlen des Ideals in der Form $px + (b + \sqrt{m})y$ darstellbar, wo x, y alle ganzen rationalen Zahlen durchlaufen. Betrachtet man die *Normen* aller dieser Zahlen:

$$p\left(px^2 + 2bxy + \frac{b^2 - m}{p}y^2\right),$$

so enthalten dieselben alle eine Form mit der Determinante m als Faktor. Es liegt nun der Gedanke nahe, die Form

$$px^2 + 2bxy + \frac{b^2 - m}{p}y^2$$

dem Ideal $\mathfrak{p}$, oder den unendlich vielen Normen der Idealzahlen zuzuordnen; wir wollen dies nun im einzelnen weiter durchführen.

1. Fall. *Reeller Körper* $k(\sqrt{m})$ *und* $m \equiv 2$, $m \equiv 3$, (4).

Es sei also $k(\sqrt{m})$ ein Körper mit einer Diskriminante $d = 4m$, einer Basis 1, $\omega = \sqrt{m}$ und beliebiger Klassenanzahl h. Bedeutet p eine positive rationale Primzahl, so sind für das Verhalten dieser Zahl p im Körper $k(\sqrt{m})$ drei Möglichkeiten denkbar:

*) Entweder es ist $\left(\frac{d}{p}\right) = -1$, dann bleibt (p) auch ein Primideal in $k(\sqrt{m})$. Wenn aber p in diesem Körper unzerlegbar ist, so heißt das, daß die Zahl p durch keine Form $x^2 - my^2$ darstellbar ist. Hieraus folgt noch ferner, daß p überhaupt durch keine quadratische Form: $ax^2 + 2bxy + cy^2$, mit der Determinante $m = b^2 - ac$ darstellbar sein kann. In der Tat sind wegen $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1$ die äußeren Koeffizienten a und c prim zu p; falls nun die Gleichung $\pm p = ax^2 + 2bxy + cy^2$ lösbar wäre, so müßte auch $\pm ap = (ax + by)^2$

$-my^2$ sein, und das ist wiederum wegen der Voraussetzung $\left(\frac{m}{p}\right) = -1$ nicht möglich.

**) Oder es ist $\left(\frac{d}{p}\right) = +1$, dann zerfällt (p) im Körper $k(\sqrt{m})$ in das Produkt zweier Hauptideale bezw. zweier Nichthauptideale;

oder es ist $\left(\frac{d}{p}\right) = 0$, dann ist (p) in $k(\sqrt{m})$ gleich dem Quadrat eines ambigen Primideals.

Hauptideale und Hauptformen.

Wenn (p) in das Produkt zweier Hauptideale zerfällt, wenn also

$$(p) = (a + b\omega)(a + b\omega') \tag{1}$$

ist, so kann man ebensogut sagen, daß die Zahl p durch eine der beiden folgenden quadratischen Formen, ev. durch die beiden Formen:

$$f = x^2 - my^2, \tag{I}$$

$$f = -x^2 + my^2, \tag{II}$$

darstellbar ist, indem man für x und y zwei ganze rationale, relativ und zu p prime Zahlen $x = a$, $y = b$ setzt.

Ist die Norm der Grundeinheit ε des Körpers $k(\sqrt{m})$ gleich $+1$, d. h. $n(\varepsilon) = +1$, so folgt aus der Idealgleichung (1) nur *eine* der beiden Gleichungen:

$$p = a^2 - mb^2 \quad \textit{oder} \quad -p = a^2 - mb^2.$$

Ist dagegen $\varepsilon = r + s\sqrt{m}$ und $n(\varepsilon) = -1$, und wird für zwei bestimmte Zahlen a, b nach Gleichung (1) etwa:

$$p = a^2 - mb^2, \tag{2}$$

so ist alsdann:

$$-p = (a^2 - mb^2)(r^2 - ms^2).$$

Da man nun die rechte Seite der letzten Gleichung als Norm einer ganzen Zahl aus $k(\sqrt{m})$ schreiben kann:

$$(a^2 - mb^2)(r^2 - ms^2) = n\left(ar + bsm + (as + br)\sqrt{m}\right),$$

oder

$$-p = (ar + bsm)^2 - m(as + br)^2,$$

so wird p und $-p$ durch eine und dieselbe quadratische Form (I) und (II) darstellbar.

Gilt nämlich die Gleichung (2), also $+p = a^2 - mb^2$, und setzt man erstens $x = a$, $y = b$, zweitens $x = ar + bsm$, $y = as + br$ in (I) ein, dann erhält man $+p$ resp. $-p$. Setzt man dieselben Wertepaare in (II) ein, dann erhält man gerade vertauscht $-p$ und $+p$.

Andererseits geht unter der Voraussetzung $n(\varepsilon) = r^2 - ms^2 = -1$ die Form (II) in die Form (I) über durch die Transformation mit der Determinante $+1$:

$$\left.\begin{aligned} x_1 &= rx + msy \\ y_1 &= -sx - ry \end{aligned}\right\}. \tag{3}$$

Denn es wird nun:

$$-x_1 + my_1^2 = -(r^2 - ms^2)(x^2 - my^2) = x^2 - my^2.$$

Wenn es umgekehrt eine Transformation mit der Determinante ± 1 gibt, welche die Formen (I) und (II) ineinander überführt, so sind gleichzeitig $+p$ und $-p$ sowohl durch $x^2 - my^2$ als auch durch $-x^2 + my^2$ darstellbar. Ist etwa $+p = a^2 - mb^2$, $-p = a_1^2 - mb_1$, so gelten notwendig Gleichungen von der Form:

$$(a + \sqrt{m}\, b) = (a_1 + \sqrt{m}\, b_1),$$

und aus dieser Idealgleichung folgt, daß $\varepsilon = \dfrac{a + \sqrt{m} b}{a_1 + \sqrt{m} b_1}$ eine Einheit in $k(\sqrt{m})$ darstellt, für welche $n(\varepsilon) = -1$ ist.

Die Formen (I) und (II) sind Formen mit der Determinante m, und es ist nun offenbar erlaubt, folgende Festsetzung zu treffen:

Wenn $\mathfrak{p} = (a + b\sqrt{m})$, *oder* $\mathfrak{p}' = (a - b\sqrt{m})$ *ein Haupt- und Primideal des Körpers* $k(\sqrt{m})$ *ist, und wenn* ε *die Grundeinheit dieses Körpers bezeichnet, so soll den Idealen* $\mathfrak{p}$, $\mathfrak{p}'$

A) *die eigentlich primitive quadratische Form* $x^2 - my^2$ *zugeordnet werden, wenn* $n(\varepsilon) = -1$ *ist;*

B) *die zwei eigentlich primitiven nicht äquivalenten Formen* $x^2 - my^2$ *und* $-x^2 + my^2$ *zugeordnet werden, wenn* $n(\varepsilon) = +1$ *ist.*

Durch eine solche Form $x^2 - my^2$ sind außer der Zahl p noch unendlich viele Zahlen darstellbar, welche prim sind zu p oder zu irgend einer gegebenen Zahl.

Setzt man nun in den Formeln (I) resp. (II):

$$x = rx_1 + sy_1,$$
$$y = tx_1 + uy_1,$$

und wählt r, s, t, u als ganze rationale Zahlen derart, daß

$$ru - st = +1$$

wird (was auf unendlich viele Weisen möglich ist), so ergeben sich aus den beiden quadratischen Formen zwei unendliche Systeme von quadratischen Formen:

$$(r^2 - mt^2)x_1^2 + 2(rs - mtu)x_1y_1 + (s^2 - mu^2)y_1^2 \tag{Ia}$$

und

$$-(r^2 - mt^2)x_1^2 - 2(rs - mtu)x_1y_1 - (s^2 - mu^2)y_1^2, \qquad \text{(IIa)}$$

oder abgekürzt geschrieben:

$$Ax^2 + 2Bxy + Cy^2, \qquad \text{(Ia)}$$

$$-Ax^2 - 2Bxy - Cy^2. \qquad \text{(IIa)}$$

Für diese Formen wird die Determinante ebenfalls:

$$D = B^2 - AC = m,$$

wie man mit Hilfe des Multiplikationssatzes für die Determinanten leicht erkennt. Jede Primzahl p, welche durch eine Form (I) oder (II) darstellbar ist, ist auch durch eine Form (Ia) bezw. (IIa) in ganzen rationalen Zahlen x, y darstellbar, und umgekehrt.

Im Fall $n(\varepsilon) = +1$ sind die beiden Formensysteme (Ia) und (IIa) verschieden, im Fall $n(\varepsilon) = -1$ aber sind die Formen (Ia) und (IIa) äquivalent, weil (I) und (II) äquivalent sind.

Es ist nun aber besonders wichtig, daß auch umgekehrt die folgende Behauptung richtig ist: Wenn die Primzahl $+p$ sich durch die quadratische Form:

$$F = Ax^2 + 2Bxy + Cy^2$$

mit der Determinante $D = m$ darstellen läßt, so ist diese Form der früheren Form (I), ev. den Formen (I) und (II) äquivalent.

Nach der Voraussetzung, daß die Determinante $m = B^2 - AC$ keinen quadratischen Faktor besitzen soll, dürfen offenbar die drei Koeffizienten A, B, C der Form F keinen gemeinsamen Faktor > 1 enthalten. Man darf ferner annehmen, daß irgend einer der drei Koeffizienten von F, z. B. der erste Koeffizient A zu einer gegebenen Zahl, speziell zu der Primzahl p prim ist. Diese Annahme enthält keine Beschränkung der Allgemeinheit; denn falls A nicht prim ist zu p, kann man aus F eine ihr äquivalente Form ableiten, deren erster Koeffizient zu A prim ist. Ist nämlich A teilbar durch p, aber C prim zu p (dies trifft zum Voraus für $p = 2$ zu), so braucht auf F nur eine Einheitstransformation von der Form:

$$x = px_1 + sy_1, \quad y = qx_1 + uy_1$$

ausgeübt zu werden, wobei q prim zu p ist. Wenn jedoch auch C durch p teilbar wäre, so wähle man eine Einheitstransformation:

$$x = q_1x_1 + sy_1, \quad y = q_2x_1 + uy_1,$$

bei welcher q_1 und q_2 zu p prim sind.

Sind x_1, y_1 zwei ganze rationale teilerfremde Zahlen, welche die Gleichung:

$$p = Ax_1^2 + 2Bx_1y_1 + Cy_1^2 \tag{4}$$

befriedigen, so ist:

$$Ap = (Ax_1 + By_1)^2 - my_1^2, \tag{5}$$

d. h. aber es ist die Zahl Ap durch die Form $x^2 - my^2$ (indem man $x = Ax_1 + By_1$, $y = y_1$ setzt) darstellbar. Aus der Gleichung (4) erkennt man leicht, daß einerseits y_1 prim zu p ist, und daß A und y_1 keinen Faktor > 1 gemeinsam haben können. Es sind daher wegen Gleichung (5) $Ax_1 + By_1$ und y_1 relativ prim zu Ap. Gilt für p die Darstellung $p = x^{*2} - my^{*2}$ durch zwei teilerfremde Zahlen x^*, y^*, so folgt in allen Fällen aus der Idealgleichheit:

$$(Ax_1 + By_1 + \sqrt{m}y_1)(Ax_1 + By_1 - \sqrt{m}y_1)$$
$$= (A)(x^* + \sqrt{m}y^*)(x^* - \sqrt{m}y^*),$$

daß (A) gleich dem Produkt zweier Hauptideale, oder daß $+ A$ durch die Form (I) darstellbar ist. In der Tat muß ja der Faktor $(x^* + \sqrt{m}y^*)$ und ebenso $(x^* - \sqrt{m}y^*)$ als Primideal in einem der Faktoren links aufgehen. Aus der Beschaffenheit der Zahlen $Ax_1 + By_1$, y_1, x^*, y^*, die zu Ap resp. p prim sind, folgt ferner, daß die Darstellung $A = x^2 - my^2$ stets durch zwei teilerfremde zu A prime Zahlen $x = r$, $y = t$ geleistet werden kann.

Seien darum r und t zwei relativ prime ganze rationale Zahlen, welche der Gleichung genügen:

$$+ A = r^2 - mt^2, \tag{6}$$

so bestimme man zwei (rationale) Zahlen s, u entsprechend den Bedingungen:

$$ru - ts = + 1 \tag{7}$$

$$- tmu + rs = B, \tag{8}$$

also derart, daß:

$$u = \frac{Bt + r}{A}, \quad s = \frac{Br + tm}{A} \tag{9}$$

wird. Alsdann ist, wegen $B^2 - m = AC$:

$$s^2 - mu^2 = \frac{1}{A^2}(B^2 - m)(r^2 - mt^2) = C \tag{10}$$

eine ganze rationale Zahl.

Bezeichnen x^*, y^* wieder wie oben zwei ganze teilerfremde Zahlen, welche der Bedingung genügen:

$$p = x^{*2} - my^{*2},$$

so wird $Ap = (r^2 - mt^2)(x^{*2} - my^{*2})$, oder:

$$Ap = [rx^* + tmy^* + (ry^* + tx^*)\sqrt{m}][rx^* + tmy^* - (ry^* + tx^*)\sqrt{m}]. \tag{11}$$

Aus den Gleichungen (11) und (5) zusammen folgt daher, daß man die ganzen Zahlen x_1, y_1 so wählen darf, daß

$$Ax_1 + By_1 = rx^* + tmy^*, \quad -y_1 = tx^* + ry^*$$

wird, und daraus berechnet man:

$$x^* = rx_1 + sy_1, \quad y^* = -tx_1 - uy_1. \tag{12}$$

Hierin sind nach Voraussetzung x_1, y_1, x^*, y^*, r und t ganze Zahlen, folglich sind auch sy_1 und uy_1 ganz; es können also s und u nur solche Nenner besitzen, welche in y_1 aufgehen. Oder mit Rücksicht auf die Gleichung (9): die rationalen Zahlen s und u können als Nenner nur solche Zahlen enthalten, die gemeinsame Faktoren von A und y_1 sind. Da diese Zahlen aber, wie gezeigt wurde, teilerfremd sind, so müssen s, u ganze Zahlen sein.

Nun stellen die beiden Gleichungen:

$$x = rx_1 + sy_1, \quad y = -tx_1 - uy_1$$

eine Substitution mit der Substitutionsdeterminante $+1$ vor, durch welche die Form (I) in $Ax_1^2 + 2Bx_1y_1 + Cy_1^2$ übergeführt wird. Die Behauptung ist damit bewiesen. Auf die gleiche Weise könnte man auch zeigen, daß die Form II äquivalent ist mit irgend einer anderen Form von der Determinante m, durch welche die Zahl $-p$ darstellbar ist.

Man kann dieselben Resultate auch so ableiten, daß man von der Form $\mathfrak{p} = (p, b + \sqrt{m})$ der Hauptideale ausgeht und dann wie im folgenden Fall verfährt.

Beliebige Primideale und Formen.

Es sei jetzt ferner p irgend eine Primzahl, für welche $\left(\frac{d}{p}\right) = +1$ oder $\left(\frac{d}{p}\right) = 0$ ausfällt, und es zerfalle (p) in $k(\sqrt{m})$ in das Produkt zweier Ideale ersten Grades, Hauptideale bezw. Nichthauptideale, oder es sei (p) gleich dem Quadrat eines Ideals, dann kann man jedenfalls schreiben:

$$(p) = \mathfrak{p} \cdot \mathfrak{p}' = (p, b + \sqrt{m})(p, b - \sqrt{m}),$$

indem wir dabei b als eine *positive* Zahl (ev. gleich 0) voraussetzen.

Analog wie oben können dann den Idealen $\mathfrak{p}$ und $\mathfrak{p}'$ Formen mit der Determinante $D = m$ zugeordnet werden.

Per Definition sollen dem Ideal $\mathfrak{p}$ die Formen entsprechen:

$$f = \frac{1}{p}(px + by + \sqrt{m}\,y)(px + by - \sqrt{m}\,y),$$

d. h.

$$f = \quad px^2 + 2bxy + \frac{b^2 - m}{p} y^2, \tag{I}$$

oder

$$f = -px^2 - 2bxy - \frac{b^2 - m}{p} y^2, \tag{II}$$

und dem Ideal $\mathfrak{p}'$ die Formen:

$$f = \quad px^2 - 2bxy + \frac{b^2 - m}{p} y^2, \tag{III}$$

oder

$$f = -px^2 + 2bxy - \frac{b^2 - m}{p} y^2. \tag{IV}$$

Zu dieser Zuordnung ist zu bemerken, daß die sämtlichen Formen eigentlich primitiv sind, indem die drei Koeffizienten keinen gemeinsamen Teiler haben, ferner:

a) Die Formen (I) und (III) einerseits, sowie (II) und (IV) andererseits gehen durch eine Transformation

$$x = x_1, \quad y = -y_1$$

mit der Transformationsdeterminante $\Delta = -1$ ineinander über und sind deshalb *uneigentlich äquivalent.*

b) Für bestimmte ganze Zahlen x, y ergeben die Formen (I) und (II) oder (III) und (IV) gleiche Zahlen mit entgegengesetzten Vorzeichen.

Im Falle die Norm der Grundeinheit ε des Körpers $k(\sqrt{m})$ gleich -1 ist, aber auch nur dann sind jedesmal die Formen (I) und (II), sowie (III) und (IV) uneigentlich äquivalent. Setzt man nämlich $\varepsilon = r + s\sqrt{m}$, dann ist:

$$x = (r - bs)x_1 - \frac{b^2 - m}{p} sy_1$$

$$y = +psx_1 + (r + bs)y_1,$$

eine Transformation mit ganzzahligen rationalen Koeffizienten und der Determinante -1, durch welche die Form (I) in die Form (II) und die Form (III) in die Form (IV) übergeführt wird. Man kann nun die Bemerkungen unter a) und b) zusammenfassen, indem man sagt:

Falls $n(\varepsilon) = -1$ ist, sind die Formen (I) und (IV), sowie (II) und (III) *eigentlich äquivalent,* und die Form $\left\{\begin{matrix}\text{(I)}\\ \text{(IV)}\end{matrix}\right.$ ist den Formen (II) und (III) uneigentlich äquivalent.

c) Im Falle $\mathfrak{p}$ ein ambiges Ideal ist, also wenn die Gleichung gilt:

$$(p, b + \sqrt{m}) = (p, b - \sqrt{m}) = (p, b + \sqrt{m}, b - \sqrt{m}),$$

lassen sich zwei *ganze* Zahlen r_1, s_1 so finden, daß $pr_1 + (b + \sqrt{m})s_1 = b - \sqrt{m}$ ist, woraus $s_1 = -1$ und $pr_1 - b = b$, also $r_1 = \frac{2b}{p}$ folgt.

Dann geht die Form (III) aus der Form (I) durch die Substitution:

$$x = x_1 - \frac{2b}{p} y_1, \quad y = y_1,$$

mit der Determinante $\Delta = +1$, hervor. Die Formen (I) und (III) sind unter dieser Voraussetzung äquivalent, und ebenso sind (II) und (IV) äquivalent.

Wenn nun zunächst $n(\varepsilon) = +1$ ist, so sollen im vorliegenden Fall nur die Formen (I) und (II) beibehalten werden, wenn aber $n(\varepsilon) = -1$ ist, folgt aus b) und c) zusammen, daß alle vier angeschriebenen Formen (I) bis (IV) äquivalent sind und durch eine einzige unter ihnen, etwa (I), ersetzt werden können.

Die Form (I) ist der Form (III) zugleich eigentlich und uneigentlich äquivalent, also ist sie *sich selbst auch uneigentlich* äquivalent. Sie geht in der Tat durch die Substitution $x = x_1 + \frac{2b}{p} y_1$, $y = -y_1$, mit der Determinante $\Delta = -1$, in sich über. Solche Formen, welche wie die Formen (I), oder (II) bis (IV) in dem jetzt betrachteten Fall, sich selbst eigentlich und uneigentlich äquivalent sind, heißen zweiseitige oder ambige Formen (nach Dedekind) oder formae ancipites (nach Gauß).

d) Ist schließlich $\mathfrak{p}$ ein Hauptideal, so hat man den schon oben erledigten Fall: es sind *gleichzeitig* jedesmal die Formen (I), (III), sowie (II), (IV) einer der Formen $x^2 - my^2$ resp. $-x^2 + my^2$ (ev. beiden Formen) äquivalent. Folglich ist wieder die Form (I) der Form (III) zugleich eigentlich und uneigentlich äquivalent, daher sind beide Formen sich selbst uneigentlich äquivalent.

Die Formen (I) und (II) sind also auch in diesem Fall ambige Formen.

Aus den Formen (I) bis (IV) lassen sich unendlich viele andere äquivalente Formen ableiten, indem man auf dieselben eine Transformation:

$$x = rx_1 + sy_1$$
$$y = tx_1 + uy_1$$

ausübt, so daß $ru - st = +1$ wird, was eben auf unendlich viele Weisen möglich ist.

Im allgemeinsten Falle erhält man hierdurch vier Formensysteme,

in speziellen Fällen zwei oder auch nur eins. Eine rationale Zahl $\pm z$, welche durch eine der Formen (I) bis (IV) darstellbar ist, ist auch durch jede zu ihr äquivalente Form darstellbar.

Umgekehrt läßt sich jetzt wieder zeigen: irgend eine Form mit der Determinante $D = m$:

$$f = Ax^2 + 2Bxy + Cy^2,$$

durch welche die (positive oder negative) Primzahl p eigentlich darstellbar ist, indem statt x, y zwei teilerfremde Zahlen x_1, y_1 gesetzt werden, muß einer der Formen (I) bis (IV) äquivalent sein.

Wenn nämlich z. B. die Gleichung gilt:

$$+p = Ax_1^2 + 2Bx_1y_1 + Cy_1^2,$$

so lassen sich zu den teilerfremden Zahlen x_1, y_1 zwei andere ganze rationale Zahlen s und u so bestimmen, daß:

$$x_1u - y_1s = +1$$

wird. Nun führt die Substitution:

$$x = x_1x' + sy'$$
$$y = y_1x' + uy',$$

die Form f über in:

$$F = +px'^2 + 2\{(Ax_1 + By_1)s + (Bx_1 + Cy_1)u\}x'y'$$
$$+ (As^2 + 2Bsu + Cu^2)y'^2,$$

oder wenn hierin die Koeffizienten anders geschrieben werden, in:

$$F = +px'^2 + 2b_1x'y' + c_1y'^2.$$

Die Determinante dieser Form ist nach den allgemeinen Sätzen über die Transformation der Formen und wie man leicht auch direkt berechnen kann, gleich m; daraus ergibt sich:

$$c_1 = \frac{b_1^2 - m}{p}, \quad \text{oder} \quad b_1^2 - m \equiv 0, (p);$$

es ist also b_1 eine ganze rationale Zahl, welche der Kongruenz $X^2 - m \equiv 0, (p)$ genügt. Bei der Untersuchung allgemeiner Ideale (S. 208) wird noch gezeigt werden, daß die Zahl b_1 nach dem Modul p nur von den Werten x_1, y_1 abhängig ist, dagegen unabhängig von den speziell gewählten Werten u, s.

Derselben Kongruenz genügt aber auch die Zahl b, und da die Kongruenz zwei mod (p) verschiedene Wurzeln, oder falls $m \equiv 0, (p)$ ist, nur eine einzige Wurzel besitzt, so ist $b_1 = \pm b + ep$, wenn e eine ganze positive oder negative Zahl bezeichnet. Ersetzt man daher in F die Veränderlichen x', y' durch: $x' = X - eY$, $y' = Y$, so erhält man statt F:

$$F_1 = pX^2 \pm 2bXY + (pe^2 + c_1)Y^2,$$

bezw., weil ja $b^2 - p(pe^2 + c_1) = b^2 - pc = m$ ausfällt:

$$F_1 = pX^2 \pm 2bXY + \frac{b^2 - m}{p} Y^2.$$

Dies ist also Form (I) oder (III), welche den Idealen $\mathfrak{p}$, $\mathfrak{p}'$ zugeordnet sind.

Faßt man die bisherigen Betrachtungen zusammen, so erhält man die folgenden Festsetzungen, welche die früher getroffenen umfassen:

Wenn $\mathfrak{p} = (p, b + \sqrt{m})$ *bezw.* $\mathfrak{p}' = (p, b - \sqrt{m})$ *ein beliebiges Primideal des Körpers* $k(\sqrt{m})$ *darstellt, wobei b positiv (oder gleich Null) vorausgesetzt ist, so sollen den Idealen* $\mathfrak{p}$ *resp.* $\mathfrak{p}'$

A) *die quadratischen Formen* (I), (II) *resp.* (III), (IV) *zugeordnet werden, wenn* $n(\varepsilon) = +1$ *ist und wenn* $\mathfrak{p}$ *weder ein ambiges noch ein Hauptideal bezeichnet;*

B) *die quadratische Form* (I) *resp.* (III) *zugeordnet werden, wenn* $n(\varepsilon) = -1$ *ist und* $\mathfrak{p}$ *weder ein ambiges noch ein Hauptideal bezeichnet.*

Ist aber $\mathfrak{p}$ *ein ambiges oder ein Hauptideal, so fallen in diesen Zuordnungen einerseits* (I), (III), *andererseits* (II), (IV) *zusammen und sind ambige Formen.*[1])

Wählt man als Ausgang ein Einheitsideal $(1, \omega)$, so führt dieser selbe Satz auf die den Hauptidealen zugeordneten Formen.

[Anmerkung. Es wäre durchaus nicht notwendig, bei der Zuordnung von quadratischen Formen und Idealen von der Normalbasis $p, b + \omega$ des Ideals auszugehen, man könnte ebenso gut von irgend einer ganz bestimmten Basis des Ideals ausgehen.

Ist $\mathfrak{p}$ ein Primideal, das in der Primzahl p aufgeht, und bilden $\pi = a_1 + b_1\omega$, $\pi_1 = c_1 + d_1\omega$ eine Basis des Ideals, so würde man statt der vier Formen (I) bis (IV) vier analoge Formen bekommen, von denen die der Form (I) oder (III) entsprechende die folgende ist:

$$F = \frac{1}{p}[(a_1x + c_1y) + (b_1x + d_1y)\omega][(a_1x + c_1y) - (b_1x + d_1y)\omega],$$

oder

$$F = \frac{a_1^2 - b_1^2 m}{p} x^2 + 2\frac{a_1c_1 - b_1d_1m}{p} xy + \frac{c_1^2 - d_1^2 m}{p} y^2. \qquad \text{(Ia)}$$

Die Koeffizienten dieser Form sind drei ganze teilerfremde Zahlen, da $a_1^2 - b_1^2 m$, $c_1^2 - d_1^2 m$, $a_1c_1 - b_1d_1m$ rationale Zahlen des Ideals $\mathfrak{p}$

1) Wenn man an Stelle des gewöhnlichen Äquivalenzbegriffes der Ideale die engere Fassung (s. S. 173 u. 328) wählt, so könnte man offenbar die Zuordnung noch bestimmter machen. Die Formen I und II würden dann verschiedenen Idealen entsprechen, wenn sie nicht äquivalent sind.

sind, und die ersten beiden Zahlen nach Voraussetzung nur durch p^1 teilbar sein dürfen. Ferner ist die Determinante der Form $D = m$. Denn da π, π_1 eine Basis des Ideals $\mathfrak{p}$ ist, so gibt es vier ganze rationale Zahlen r, s, t, u von der Art, daß $ru - st = \pm 1$ ist und daß

$$\pi = rp + t(b + \omega) \quad \text{und} \quad \pi_1 = sp + u(b + \omega)$$

wird. Die Form F kann man daher auch schreiben:

$$F = \frac{1}{p} \cdot n[p(rx + sy) + (tx + uy)b + (tx + uy)\omega],$$

woraus zu ersehen ist, daß die Form (Ia) durch eine Transformation:

$$x = rx_1 + sy_1, \quad y = tx + uy$$

in die Form (I) oder (III) übergeführt werden kann, d. h. einer dieser Formen äquivalent ist, je nachdem $rs - tu$ gleich $+1$ oder -1 ausfällt; folglich ist auch die Determinante der Form F gleich m. Man erhält somit den Satz:

Den verschiedenen Zahlenpaaren, welche eine Basis des Ideals $\mathfrak{p}$ *bilden können, entsprechen Formen mit der Determinante* m, *welche untereinander eigentlich oder uneigentlich äquivalent sind.*

D. h. die Abhängigkeit verschiedener Paare von Basiszahlen voneinander führt auf die Äquivalenz der entsprechenden Formen.]

Beliebige Ideale und Formen.

Sei schließlich $\mathfrak{j} = (\iota_1, \iota_2)$ ein beliebiges Ideal, nicht nur ein Primideal, und es sei $\mathfrak{j}$ nicht durch eine rationale Zahl teilbar, so kann man stets $\iota_1 = a$ und $\iota_2 = b + \omega$ setzen, wenn a die absolut kleinste rationale Zahl in $\mathfrak{j}$ bedeutet. In der Tat, wäre a, $b + c\omega$ eine Basis des Ideals, so können a, b, c keinen gemeinsamen rationalen Faktor besitzen, weil sonst auch das Ideal $\mathfrak{j}$ selbst diesen Faktor besäße. Alsdann lassen sich drei ganze rationale Zahlen x^*, y^*, z^* so bestimmen, daß $a\omega x^* + by^* + c\omega y^* + cmz^* + bz^*\omega$ von der Form $B + \omega$ wird, woraus die Richtigkeit der Behauptung folgt. Nun sei $\mathfrak{j} = (a, b + \sqrt{m})$, so sollen den Idealen $\mathfrak{j}$ und $\mathfrak{j}'$ im allgemeinen wieder vier (d. h. je zwei) Formen mit der Determinante m zugeordnet werden, analog den Formen (I) bis (IV) auf S. 203. Dem Ideal $\mathfrak{j}$ entspricht z. B., analog der Form (I), die Form

$$f = ax^2 + 2bxy + \frac{b^2 - m}{a} \cdot y^2$$

usw.

Während nun ohne weiteres klar ist, daß die Zahl $\pm a$ durch die Form f und die drei übrigen, sowie durch jede Form darstellbar

ist, welche *einer dieser vier Formen äquivalent ist*, so läßt sich jetzt nicht umgekehrt beweisen, daß jede Form der Determinante m, durch welche $\pm a$ darstellbar ist, stets einer der vier zu j und j' zugeordneten Formen äquivalent sein muß.

Einmal gibt es ja außer dem Ideal j im allgemeinen noch andere Ideale mit der Norm a, die nicht einmal dem Ideal j äquivalent zu sein brauchen, und aus jedem dieser Ideale läßt sich ein neues Quadrupel von quadratischen Formen ableiten. Ist andererseits

$$F = Ax^2 + 2Bxy + Cy^2$$

eine quadratische Form mit der Determinante m, durch welche sich z. B. die Zahl $+a$ mittels der relativ primen Zahlen x_1, y_1 darstellen läßt:

$$a = Ax_1^2 + 2Bx_1y_1 + Cy_1^2,$$

und bestimmt man zwei ganze rationale Zahlen s, u derart, daß $x_1u - y_1s = 1$ wird, so führt die Einheitstransformation:

$$x = x_1X + sY$$
$$y = y_1X + uY,$$

die Form F in die ihr äquivalente Form:

$$F' = aX^2 + 2b_1XY + c_1Y^2,$$

über. Die Form F' kann aber, wie man sich leicht überzeugt, der Form f nur äquivalent sein, wenn $b_1 \equiv b$, (a) ist. Um die Frage entscheiden zu können, ob F' und f äquivalent sind, ist nun vor allem wichtig, daß man weiß, wie die Zahl b_1 von den Größen x_1, y_1, u, s abhängt.

Die Determinante der Form F' ist $b_1^2 - ac_1 = m$, es ist daher b_1 eine Wurzel der quadratischen Kongruenz $x^2 - m \equiv 0$, (a). Eine solche Kongruenz kann eine oder zwei, mod (a) verschiedene Wurzeln haben, wenn a eine Primzahl ist, sie kann aber mehr als zwei verschiedene Wurzeln haben, wenn a eine zusammengesetzte Zahl ist. Wir wollen nun zeigen, daß der Koeffizient b_1 Modulo a nur abhängig ist von den Werten x_1, y_1 und sich mod (a) nicht ändert, wenn man für s, u irgend ein anderes Lösungssystem der unbestimmten Gleichung $x_1u - y_1s = 1$ setzt. Die Diophantische Gleichung $x_1u - y_1s = 1$ besitzt unendlich viele Lösungen. Seien s, u und s_1, u_1 zwei solche Lösungen, so ist offenbar $x_1(u - u_1) - y_1(s - s_1) = 0$, oder $u - u_1 = ky_1$ und $s - s_1 = kx_1$, falls k einen Proportionalitätsfaktor bezeichnet. Für den mittleren Koeffizienten in F' ergeben sich dann:

$$b_1 = Ax_1s + B(x_1u + y_1s) + Cy_1u,$$

resp.:

$$b_2 = Ax_1s_1 + B(x_1u_1 + y_1s_1) + Cy_1u_1,$$

und hieraus folgt durch einfache Subtraktion und die Substitution $u - u_1 = k \cdot y_1$, $s - s_1 = k \cdot x_1$:

$$b_1 - b_2 \equiv 0, \ (a).$$

Zwischen dem Koeffizienten b_1 und den Größen x_1, y_1 besteht daher eine in einem bestimmten Sinne eindeutige Beziehung, und man kann nach einer von Gauß analog gebrauchten Ausdrucksweise sagen, daß die Darstellung der Zahl a durch die Form F mittels der Größen x_1, y_1 zu der bestimmten Kongruenzwurzel b_1 der Kongruenz $x^2 - m \equiv 0, \ (a)$ gehört.

Man erhält daher den Satz:

Die Form F ist dann und nur dann der Form f äquivalent, wenn die Darstellung der Zahl a durch F zur Kongruenzwurzel b gehört.

Wenn schließlich $\mathfrak{j}$ ein Ideal bezeichnet, welches durch eine rationale Zahl s teilbar ist, so führt man zuerst die Division $\frac{\mathfrak{j}}{s}$ aus und ordnet dem vereinfachten Ideal eine Form mit der Determinante $D = m$ zu.

Die Zuordnung der Formen und Ideale läßt sich auch umkehren: einer primitiven quadratischen Form $ax^2 + 2bxy + cy^2$ von der Determinante m soll das Ideal: $(a, b + \sqrt{m})$ des Körpers entsprechen Äquivalenten Formen kann man alsdann ein und dasselbe Ideal zuordnen. (Vergl. S. 219.)

2. Fall. *Imaginärer Körper* $k(\sqrt{m})$ *und* $m \equiv 2$, $m \equiv 3$, (4). Es sei also wieder $d = 4m$ die Diskriminante, $1, \omega = \sqrt{m}$ die Basis des Körpers und seine Klassenanzahl $h \geqq 1$.

Ist p eine rationale Primzahl, für welche $\left(\frac{d}{p}\right) = -1$ ausfällt, welche also im Körper $k(\sqrt{m})$ nicht zerfällt, dann ist die Zahl p überhaupt durch keine quadratische Form mit der Determinante $D = m$ darstellbar.

Wenn nun $f = ax^2 + 2bxy + cy^2 = \frac{1}{a}[(ax + by)^2 - my^2]$ eine Form mit der negativen Determinante m ist, so müssen offenbar a und c *gleiches* Vorzeichen besitzen, und es stellt f entweder nur *positive* oder nur *negative* Zahlen dar, je nachdem a, c positiv oder negativ sind. Man bezeichnet eine Form mit positiven [negativen] äußeren Koeffizienten a, c als eine positive [negative] Form mit der negativen Determinante m. Es genügt nun, wenn man bei der Betrachtung

der quadratischen Formen einer negativen Determinante nur die Formen einer Art, etwa die positiven, beibehält, da die beiden Arten vollständig getrennt sind, sich aber übrigens genau gleich verhalten.

Verfährt man demgemäß bei der Zuordnung von Idealen und Formen, so ergibt sich gegen den ersten Fall als einzige Änderung die, daß man sich von vornherein auf die Formen (I) und (III) von Seite 203 beschränkt.

3. Fall. Wenn $k(\sqrt{m})$ *ein reeller Körper* ist, dessen Grundzahl m die Bedingung $m \equiv 1, (4)$ erfüllt, und wenn man in der bisherigen Weise den Idealen quadratische Formen zuordnet, so erhält man zunächst nicht den Anschluß an die von Gauß geschaffene Theorie.

Es sei $k(\sqrt{m})$ ein solcher reeller Körper, als dessen Basis $1,\ \omega = \frac{1+\sqrt{m}}{2}$ angenommen werde und dessen Diskriminante $d = m$ ist. Dann würden nach den früheren Festsetzungen z. B. einem Haupt- und Primideal ersten Grades $\mathfrak{p} = (a + b\omega)$ Formen zugeordnet sein, wie die folgende:

$$f = x^2 + xy + \frac{1-m}{4} y^2.$$

Diese Formen entsprechen aber nicht der von Gauß und anderen Mathematikern stets festgehaltenen Bedingung, daß der mittlere Koeffizient *gerade* ist. Während ferner im ersten und zweiten Fall die Determinante der Formen $D = m = \frac{1}{4} d$ war, würde sich nun

$$D = \frac{1}{4} - \frac{1-m}{4} = \frac{m}{4},$$

also als eine gebrochene Zahl, ergeben.

Historische Gründe rechtfertigen den Wunsch, den Idealen des Körpers $k(\sqrt{m})$ auch Formen von der Determinante m, entsprechend der Gaußschen Theorie, gegenüberzustellen.

Ehe wir uns jedoch der Lösung dieser Aufgabe zuwenden, müssen wir noch eine Bemerkung vorausschicken über die Beschaffenheit der Koeffizienten a, b, c der Formen mit der Determinante $D = m$ und über die durch solche Formen dargestellten Zahlen.

Wenn $f = ax^2 + 2bxy + cy^2$ eine quadratische Form mit der Determinante $D = b^2 - ac (\equiv 1, (4))$ ist und wenn die Koeffizienten $a, 2b, c$ teilerfremd sind, insbesondere nicht den Faktor 2 gemeinsam haben, so kann durch f keine schlechthin gerade Zahl, d. h. keine Zahl, welche den Faktor 2^1 aber nicht mehr den Faktor 4 enthält,

dargestellt werden. Denn ist etwa a ein ungerader Koeffizient der Form f, dann wird

$$af = (ax + by)^2 - my^2,$$

und hieraus sieht man, daß $a \cdot f$ und folglich f selbst für ganzzahlige Werte x, y entweder ungerade ist oder aber mindestens durch 4 teilbar sein muß. Eine schlechthin gerade Zahl wäre also durch f nur darstellbar, falls a und c gerade sind, oder genauer ausgedrückt, falls a, $2b$, c den Faktor 2^1 gemeinsam haben. Für die quadratfreien Determinanten D, welche die Bedingung $D \equiv 1, (4)$ erfüllen, aber auch nur für diese gibt es nun außer den eigentlich primitiven Formen $f = ax^2 + 2bxy + cy^2$, auch solche, deren Koeffizienten a, $2b$, c durch 2^1 und keine andere Zahl teilbar sind. Nimmt man die oben angeschriebene Form f doppelt, also

$$2f = 2x^2 + 2xy + 2\,\frac{1-m}{4}\,y^2,$$

so hat man ein Beispiel einer solchen.

Formen, deren Koeffizienten a, $2b$, c den gemeinsamen Teiler 2^1 besitzen, heißen nach Gauß *uneigentlich primitive Formen* der Determinante $D = m$. Da aus einer uneigentlich primitiven Form durch eine Transformation mit ganzzahligen Koeffizienten niemals eine eigentlich primitive Form abgeleitet werden kann, so hat man bei der Aufstellung sämtlicher Formen des vorliegenden dritten Falles von vornherein die eigentlich und uneigentlich primitiven Formen zu berücksichtigen. Es bieten sich für die Zuordnung der Ideale und Formen zwei Wege dar.

Erstens kann man per def. dem Ideal $\mathfrak{p}$ anstatt f, wie oben geschehen, andere Formen zuordnen, und zwar einmal die uneigentlich primitive Form:

$$2f = 2x^2 + 2xy + 2\,\frac{1-m}{4}\,y^2,$$

sodann diejenigen eigentlich primitiven Formen mit einem geraden mittleren Koeffizienten, welche aus f (und den übrigen nach früherer Weise zugeordneten Formen) durch eine Substitution mit der Determinante 2 hervorgehen und welche voneinander und von $2f$ verschieden, d. h. einander nicht äquivalent, sind.

Um die letzteren Formen aus f abzuleiten, genügt es, die Substitutionen:

$$\text{A)}\ \begin{cases} x = x_1, \\ y = 2y_1, \end{cases} \qquad \text{B)}\ \begin{cases} x = -2y_1, \\ y = x_1, \end{cases} \qquad \text{C)}\ \begin{cases} x = x_1 + 2y_1 \\ y = -x_1 \end{cases}$$

auf die Form f auszuüben. Zusammen mit $2f$ erhält man so vier Formen, von denen nur die voneinander verschiedenen, untereinander nicht äquivalenten, beizubehalten sind als Vertreter je eines Formensystems.

Indem man für alle Ideale, Hauptideale und Nichthauptideale diese Vorschriften anwendet, erhält man lauter Formen mit der Determinante $D = m$ und einem geraden mittleren Koeffizienten.

[Anmerkung. Ich übergehe den nicht schwierigen Beweis, daß jede Substitution mit der Determinante 2 sich aus einer der oben aufgestellten Substitutionen mit der Determinante 2 und einer zweiten Substitution mit der Determinante 1 zusammensetzen läßt.

Wenn nämlich $x = r_1 x^* + s_1 y^*$, $y = t_1 x^* + u_1 y^*$ eine Substitution mit der Determinante $r_1 u_1 - s_1 t_1 = +2$, und $x^* = r x_1 + s y_1$, $y^* = t x_1 + u y_1$ eine Substitution mit der Determinante $ru - st = +1$ darstellt, so ist die kombinierte Substitution:

$$x = (r_1 r + s_1 t) x_1 + (r_1 s + s_1 u) y_1,$$
$$y = (t_1 r + u_1 t) x_1 + (t_1 s + u_1 u) y_1$$

eine solche mit der Determinante 2. Falls nun umgekehrt:

$$x = R x_1 + S y_1, \quad y = T x_1 + U y_1$$

irgend eine gegebene Substitution mit der Determinante 2 bedeutet, so lassen sich r, s, t, u als ganze rationale Zahlen mit der Bedingung $ru - st = +1$ so bestimmen, daß:

$$R = r_1 r + s_1 t$$

usw. usw. wird, wenn statt r_1, s_1, t_1, u_1 die angeschriebenen Kombinationen aus den Formeln A), oder B), oder C) gesetzt werden.]

Dieser erste, hier vorgeschlagene Weg braucht nicht weiter verfolgt zu werden. Es ist in der Tat zweckmäßiger, zur Aufstellung der uneigentlich resp. eigentlich primitiven Formen von dem im Körper $k(\sqrt{m})$ enthaltenen Ring $r(\sqrt{m})$ [vgl. S. 168 ff.] auszugehen, da man dabei mit kleinen Änderungen ganz analog verfahren kann wie in den beiden ersten Fällen.

Sei $\mathfrak{p} = (a + b\omega)$ ein Hauptideal des Körpers selbst, so setzt man statt dessen $(2)\mathfrak{p} = (2a + 2b\omega)$ und ordnet nun *diesem* Ideal die uneigentlich primitiven Formen zu:

$$f = \quad 2x^2 + 2xy + 2\frac{1-m}{4}y^2, \tag{I}$$

$$f = -2x^2 - 2xy - 2\frac{1-m}{4}y^2. \tag{II}$$

Wenn ferner $\mathfrak{p} = (a + b\sqrt{m})$ ein Hauptideal des Rings $r(\sqrt{m})$ darstellt, so ordnet man diesem Ideal die eigentlich primitiven Formen zu:

$$f = \quad x^2 - my^2, \tag{Ia}$$

$$f = -x^2 + my^2. \tag{IIa}$$

Im übrigen knüpfen sich an die Aufstellung dieser zwei Formenpaare dieselben Betrachtungen, wie wir sie eingehender im 1. Fall angestellt haben. Es sind nur noch zwei Tatsachen hier besonders zu beachten:

Zunächst sieht man leicht, daß die beiden Formen (I) und (II) ambig (zweiseitig) sind, denn sie werden durch eine Substitution $x = -x_1 - y_1$, $y = y_1$ mit der Determinante -1 in sich übergeführt.

Sodann gilt *allgemein*, daß eine eigentlich primitive Form niemals einer uneigentlich primitiven Form äquivalent sein kann, wie man durch Anwendung einer Einheitssubstitution sofort erkennt.

Die Formen (I), (II) usw. entsprechen anders ausgedrückt den Idealen $(2, 2\omega)$ des Körpers bezw. $(1, \sqrt{m})$ des Rings $r(\sqrt{m})$. Wenn nun $\mathfrak{p}$ ein beliebiges, zu (2) primes Primideal des Körpers $k(\sqrt{m})$ ist, so ordnet man den Idealen $(2)\mathfrak{p}$ und $(2)\mathfrak{p}'$ vier uneigentlich primitive Formen und dem zu $\mathfrak{p}$ gehörigen regulären Ringideal $\mathfrak{p}_r$ und $\mathfrak{p}_r'$ vier eigentlich primitive Formen zu, genau wie in den früheren Fällen.

Jedes dieser Quadrupel behandelt man dann für sich weiter, indem nun klar ist, daß der wesentliche Unterschied gegenüber früher überhaupt nur in der Einführung der zwei Arten von primitiven Formen liegt.

Schließlich unterscheidet sich der

4. Fall, wo $k(\sqrt{m})$ *ein imaginärer Körper mit der Grundzahl* $m \equiv 1, (4)$ ist, von dem vorigen dritten Fall nur dadurch, daß man sich von vornherein auf die positiven *oder* negativen Formen der Determinante $D = m$ beschränkt.

37. Multiplikation der Ideale und die Komposition der Formen.

Durch die Zuordnung von quadratischen Formen zu den Idealen und umgekehrt, wie sie im vorhergehenden Paragraphen durch Definition festgesetzt wurde, ist der Grund für die Theorie der quadratischen Formen gelegt. Es ist aber zur Entwicklung dieser Theorie nötig zu wissen, in welcher Beziehung die Formenklassen und Ideal-

klassen stehen. Diese Frage hängt eng zusammen mit der Übertragung der Multiplikation der Ideale auf die Operationen mit den Formen, die jetzt zunächst behandelt werden muß. Bei der Erledigung dieser Aufgabe wären wieder die Fälle getrennt zu behandeln, in welchen die Grundzahl des Körpers $m \not\equiv 1$, (4) oder $m \equiv 1$, (4) ist. Die einfacheren Fälle sind natürlich die, daß $m \equiv 2$, $m \equiv 3$, (4) ist, und wir wollen uns auf die Behandlung dieser Fälle beschränken. Die Diskussion der entsprechenden Fragen für $m \equiv 1$, (4) ist nicht wesentlich verschieden hiervon, der Leser möge aber nicht unterlassen, diese Ergänzung auszuführen.

Es seien $\mathfrak{p}$ und $\mathfrak{q}$ zwei verschiedene, äquivalente oder nicht äquivalente Primideale des Körpers $k(\sqrt{m})$, und es möge:

$$\mathfrak{p} = (p,\ b + \sqrt{m}), \quad \mathfrak{q} = (q,\ b_1 + \sqrt{m})$$

gesetzt werden, dann ist das Produkt $\mathfrak{p}\mathfrak{q}$ wieder ein Ideal des Körpers, welches man schreiben kann:

$$\mathfrak{p}\mathfrak{q} = (pq,\ B + \sqrt{m}).$$

Die ganze Zahl $B + \sqrt{m}$ gehört sowohl dem Ideal $\mathfrak{p}$ als auch dem Ideal $\mathfrak{q}$ an, d. h. man kann zwei ganze rationale Zahlen u bezw. v so angeben, daß

$$pu + b = B, \quad qv + b_1 = B$$

wird, und man darf auch p, $B + \sqrt{m}$ als Basiszahlen für $\mathfrak{p}$ und q, $B + \sqrt{m}$ als Basiszahlen für $\mathfrak{q}$ wählen. Daher sind u. a. den Idealen $\mathfrak{p}$, $\mathfrak{q}$ und $\mathfrak{p}\mathfrak{q}$ bezw. die folgenden Formen zugeordnet:

$$f = px^2 + 2Bxy + \frac{B^2 - m}{p} y^2, \tag{1}$$

$$f_1 = qx_1^2 + 2Bx_1y_1 + \frac{B^2 - m}{q} y_1^2, \tag{2}$$

$$F = pqX^2 + 2BXY + \frac{B^2 - m}{pq} Y^2. \tag{3}$$

Dies sind drei Formen, die ihrerseits in einer einfachen und merkwürdigen Beziehung zueinander stehen, wie sich jetzt zeigen läßt.

In der Tat, da $px + (B + \sqrt{m})y$ eine Zahl des Ideals $\mathfrak{p}$ ist und ebenso $qx_1 + (B + \sqrt{m})y_1$, ferner $pqX + (B + \sqrt{m})Y$ Zahlen der Ideale $\mathfrak{q}$ und $\mathfrak{p}\mathfrak{q}$ sind, so gilt nach dem Multiplikationssatz für Ideale eine Gleichung:

$$[px + (B + \sqrt{m})y]\,[qx_1 + (B + \sqrt{m})y_1] = pqX + (B + \sqrt{m})Y.$$

Wenn man hieraus X, Y durch Koeffizientenvergleichung berechnet zu:

$$\left.\begin{aligned} X &= xx_1 - \frac{B^2-m}{pq}yy_1 \\ Y &= pxy_1 + qx_1y + 2Byy_1, \end{aligned}\right\} \qquad (\Sigma)$$

so kann man sagen, daß die Form F durch die Substitution (Σ) in das *Produkt* der beiden Formen f und f_1 übergeht. Umgekehrt ist das Produkt der beiden Formen f und f_1 gleich F, wenn man die Veränderlichen x, y und x_1, y_1 nach der Vorschrift der Substitution (Σ) zusammenfaßt.

Auch wenn unmittelbar den Idealen $\mathfrak{p}$ und $\mathfrak{q}$ die Formen

$$\varphi = px'^2 + 2bx'y' + \frac{b^2-m}{p}y'^2$$

$$\varphi_1 = px_1'^2 + 2b_1x_1'y_1' + \frac{b_1^2-m}{q}y_1'^2$$

zugeordnet werden, kann man F als das Produkt von φ und φ_1 bezeichnen. Tatsächlich ist φ äquivalent zu f und φ_1 äquivalent zu f_1, und die Richtigkeit der Behauptung sieht man sofort ein, indem man in der Formel (Σ) einfach

$$\begin{aligned} x &= x' + uy' \\ y &= y' \end{aligned} \quad \text{bezw.} \quad \begin{aligned} x_1 &= x_1' + vy_1' \\ y_1 &= y_1' \end{aligned}$$

setzt.

Für die Multiplikation der Formen hat Gauß[1]) die Bezeichnung *Komposition* eingeführt. Die Form F heißt aus den Formen f und f_1 *komponiert*, und man kann symbolisch schreiben $F = ff_1$.

Die Komposition bleibt offenbar dieselbe, wenn $\mathfrak{p}$ und $\mathfrak{q}$ zwei ambige verschiedene Primideale sind. Ferner ist von vornherein auch selbstverständlich, wie die Formen zusammenhängen, welche den Idealen $\mathfrak{p}$ und $\mathfrak{p}^2$ zugeordnet sind. Es sei $\mathfrak{p}$ ein Primideal, welches nicht in (2) aufgeht, von der Form:

$$\mathfrak{p} = (p, B + \sqrt{m}) \quad \text{und} \quad \mathfrak{p}^2 = (p^2, B + \sqrt{m}).$$

Bedeuten dann:

$$f = px^2 + 2Bxy + \frac{B^2-m}{p}y^2$$

und

$$F = p^2X^2 + 2BXY + \frac{B^2-m}{p^2}Y^2,$$

zwei, den Idealen $\mathfrak{p}$ und $\mathfrak{p}^2$ zugeordnete Formen, so zeigt sich, wie

1) Disqu. arithm. V, S. 234 ff.

oben, daß man auch $F = f^2$ setzen darf, indem man zwischen X, Y und x, y eine Abhängigkeit durch die Substitution:

$$\left.\begin{aligned} X &= x^2 - \frac{B^2 - m}{p^2} y^2 \\ Y &= 2pxy + 2By^2 \end{aligned}\right\} \qquad (\Sigma_1)$$

annimmt.

Man bezeichnet diesen Fall als Komposition einer Form mit sich selbst, und man erkennt übrigens durch Vergleichung der Substitutionen Σ und Σ_1, daß dieser speziellere Fall direkt aus dem allgemeineren Fall ableitbar ist.

Eine solche Komposition ist nur dann nicht möglich, wenn $\mathfrak{p}$ in (2) aufgeht. Falls dagegen $\mathfrak{p}$ ein zu 2 primes ambiges Ideal ist, so kann man schreiben:

$$\mathfrak{p} = (p, \sqrt{m}) \quad \text{und} \quad \mathfrak{p}^2 = (p, p\sqrt{m}).$$

Nach den früheren Definitionen ist dann:

$$f = px^2 - \frac{m}{p} y^2,$$
$$F = X^2 - mY^2,$$

und es ist $F = f^2$, wenn man die Substitution anwendet:

$$X = px^2 + \frac{m}{p} y^2, \quad Y^2 = 2xy.$$

Schließlich ist noch die Frage zu entscheiden, wie sich zwei beliebige Formen zusammensetzen lassen, welche irgend zwei Idealen zugeordnet sind.

Es bezeichnen $\mathfrak{j}$ und $\mathfrak{j}_1$ zwei beliebige Ideale des Körpers, und zwar sei:

$$\mathfrak{j} = (a, b + c\sqrt{m}),$$
$$\mathfrak{j}_1 = (a_1, b_1 + c_1\sqrt{m}).$$

Damit die Koeffizienten der diesen Idealen zugeordneten Formen nicht einen gemeinsamen Faktor besitzen, sei *erstens* vorausgesetzt, daß die Ideale nicht durch rationale Hauptideale teilbar sind. Dazu ist notwendig, daß sowohl die Zahlen a, b, c, als auch a_1, b_1, c_1 keinen gemeinschaftlichen Teiler besitzen. Dann sind die beiden Ideale in der folgenden Weise darstellbar:

$$\mathfrak{j} = (a, b + \sqrt{m}), \quad \mathfrak{j}_1 = (a_1, b_1 + \sqrt{m}).$$

Das Produkt dieser beiden Ideale:

$$\mathfrak{j}\mathfrak{j}_1 = (aa_1, a_1 b + a_1\sqrt{m}, ab_1 + a\sqrt{m}, bb_1 + m + (b + b_1)\sqrt{m}, \ldots)$$

kann alsdann offenbar durch eine Basis:

$$aa_1, \; B+\sqrt{m}, \text{ d. h. in der Form } \mathfrak{j}\mathfrak{j}_1 = (aa_1, \; B+\sqrt{m})$$

dargestellt werden, wenn

$$a, \quad a_1, \quad b+b_1$$

keinen gemeinsamen Zahlenfaktor besitzen. Es soll jetzt *zweitens* vorausgesetzt werden, daß diese Bedingung für die Ideale $\mathfrak{j}$, $\mathfrak{j}_1$ erfüllt ist. Wenn aber diese Bedingung erfüllt ist, so kann man schreiben:

$$\mathfrak{j} = (a, \; B+\sqrt{m}), \quad \mathfrak{j}_1 = (a_1, \; B+\sqrt{m}),$$

indem man zwei ganze rationale Zahlen u, v so angeben kann, daß gleichzeitig $B = au + b = a_1 v + b_1$ ist. Entsprechen nun den Idealen $\mathfrak{j}$ und $\mathfrak{j}_1$ und $\mathfrak{j}\mathfrak{j}_1$ die Formen:

$$f = ax^2 \quad + 2Bxy \quad + \frac{B^2-m}{a} y^2,$$

$$f_1 = a_1 x_1^2 \quad + 2Bx_1 y_1 + \frac{B^2-m}{a_1} y_1^2,$$

$$F = aa_1 X^2 + 2BXY + \frac{B^2-m}{aa_1} Y^2,$$

so läßt sich F wieder als *Produkt* der Formen f und f_1 auffassen.

Aus dem Multiplikationssatz für die Ideale folgt nämlich wiederum, daß für bestimmte x, y, x_1, y_1 und X, Y die Gleichung besteht:

$$[ax + By + \sqrt{m}y][a_1 x_1 + By_1 + \sqrt{m}y_1] = aa_1 X + (B+\sqrt{m}) Y;$$

hieraus folgen durch Ausmultiplizieren der linken Seite und Vergleichung der Koeffizienten die Relationen:

$$\left.\begin{aligned} X &= xx_1 - \frac{B^2-m}{aa_1} yy_1 \\ Y &= axy_1 + a_1 x_1 y + 2Byy_1. \end{aligned}\right\} \qquad (\Sigma_2)$$

Setzt man diese Werte von X, Y in die Form F ein, so stellt sie direkt das Produkt der beiden Formen f und f_1 dar.

Ordnet man den Idealen $\mathfrak{j}$, $\mathfrak{j}_1$ statt der Formen f, f_1 die Formen

$$\varphi = ax'^2 \quad + 2bx'y' \quad + \frac{b^2-m}{a} y'^2$$

$$\varphi_1 = a_1 x_1'^2 + 2b_1 x_1' y_1' + \frac{b_1^2-m}{a_1} y_1'^2$$

zu, entsprechend den ursprünglichen Darstellungen $\mathfrak{j} = (a, b+\sqrt{m})$, und $\mathfrak{j}_1 = (a_1, b_1+\sqrt{m})$, so sind ja einerseits f und φ und andererseits f_1 und φ_1 äquivalent, und es läßt sich wieder, ganz wie es oben für die Primideale $\mathfrak{p}$ und $\mathfrak{q}$ ausgeführt wurde, F als Produkt von φ und φ_1 darstellen.

Indem man alle bisherigen Resultate zusammenfaßt, ergibt sich, daß zwei Formen mit derselben Determinante m:

$$f = ax^2 + 2bxy + cy^2$$
$$f_1 = a_1 x_1^2 + 2b_1 x_1 y_1 + c_1 y_1,$$

stets dann zu einer dritten quadratischen Form F mit der Determinante m komponiert werden können, wenn a, a_1, $b + b_1$ keinen gemeinsamen Teiler haben.

Es ist besonders zu beachten, daß nicht bloß die Form F, sondern auch jede zu F äquivalente Form F' aus denselben Formen f und f_1 zusammengesetzt werden kann.

Die bisherige Betrachtung ist auch umkehrbar: wenn eine Form F aus zwei Formen f, f_1 zusammengesetzt ist und wenn den Formen f und f_1 die Ideale $\mathfrak{j}$ resp. $\mathfrak{j}_1$ zugeordnet sind, so entspricht F dem Idealprodukt $\mathfrak{j}\mathfrak{j}_1$.

Der Fundamentalsatz der Komposition, welcher das Verhalten äquivalenter Formen betrifft, ist nach Gauß der folgende:

Satz. *Wenn sich die beiden quadratischen Formen f und f_1 zu der Form F und ebenso φ und φ_1 zu der Form Φ zusammensetzen lassen, und wenn einerseits die Formen f und φ, sowie andererseits f_1 und φ_1 äquivalent sind, so müssen auch die Formen F und Φ äquivalent sein.*

Beweis. Wenn durch die Formen f und f_1 irgend zwei Zahlen a resp. a_1 darstellbar sind, so sind diese Zahlen auch durch φ und φ_1 darstellbar, und es ist aa_1 gleichzeitig durch die Formen F und Φ darstellbar. Nach dem folgenden Satze, der aus praktischen Gründen dem eben behandelten Satze nachgeschickt ist, entsprechen nun den Formen f und φ, sowie f_1 und φ_1 jedesmal äquivalente Ideale. Wenn etwa $\mathfrak{j}$ und $\mathfrak{h}$ den Formen f und φ, ferner $\mathfrak{j}_1$ und $\mathfrak{h}_1$ den Formen f_1 und φ_1 zugeordnet sind, so ist $\mathfrak{j} \sim \mathfrak{h}$, $\mathfrak{j}_1 \sim \mathfrak{h}_1$, und es ist folglich auch $\mathfrak{j}\mathfrak{j}_1 \sim \mathfrak{h}\mathfrak{h}_1$. Den Idealen $\mathfrak{j}\mathfrak{j}_1$ und $\mathfrak{h}\mathfrak{h}_1$ entsprechen aber u. a. die Formen F und Φ, dieselben müssen eigentlich äquivalent sein, weil durch sie gleichzeitig positive oder negative Zahlen darstellbar sind.

Aus dem Zusammenhang zwischen der Komposition der Formen und der Multiplikation der Ideale ergibt sich als wichtigste Folgerung die Beziehung zwischen Formenklassen und Idealklassen auf Grund des folgenden Satzes.

Satz. *Sind $\mathfrak{j}$ und $\mathfrak{j}_1$ zwei äquivalente Ideale des Körpers $k(\sqrt{m})$, jedes derselben ohne rationale Faktoren, so sind die quadratischen For-*

men, welche per def. den Idealen zugeordnet sind, ebenfalls paarweise äquivalent.

Beweis: Man kann zunächst, ausgehend von der Komposition zweier Formen, die Äquivalenz der Formen etwas anders definieren. Lassen sich nämlich zwei Formen f und f_1 mit einer und derselben Hauptform φ $(= x^2 - my^2)$ so zusammensetzen, daß die beiden Formen $F = f \cdot \varphi$ und $F_1 = f \cdot \varphi$ einander äquivalent, oder gar gleich sind, so sind auch die Formen f und f_1 äquivalent, und umgekehrt. Denn es ist offenbar jede Zahl, welche durch f darstellbar ist, auch durch f_1, und zwar zur selben Kongruenzwurzel gehörig, darstellbar.

Nach der Voraussetzung, daß $\mathfrak{j}$ und $\mathfrak{j}_1$ äquivalente Ideale sind, gibt es zwei ganze Zahlen des Körpers α, β, von der Beschaffenheit, daß $(\alpha)\mathfrak{j} = (\beta)\mathfrak{j}_1$ ausfällt. Ist nun dem Hauptideal (α) die Hauptform φ und dem Ideal (β) daher die Form $\pm\varphi$ zugeordnet und entsprechen den Idealen $\mathfrak{j}$, $\mathfrak{j}_1$, $(\alpha)\mathfrak{j} = (\beta)\mathfrak{j}_1$ die Formen f, f_1 und F, so ist notwendig $F = \varphi \cdot f = \pm \varphi \cdot f_1$. In der Tat lassen sich die Formen φ, f einerseits und $\pm\varphi$, f_1 andererseits nach den allgemeinen Vorschriften zusammensetzen, da der Koeffizient a_1 von φ gleich 1 ist. Aus der Gleichung $\varphi \cdot f = \pm \varphi f_1$ folgt, daß die Formen f und $\pm f_1$ äquivalent sind, d. h. aber die vier Formen, welche den Idealen $\mathfrak{j}$ und $\mathfrak{j}_1$ zugeordnet sind, sind paarweise äquivalent.

Wenn ferner f und f_1 zwei äquivalente Formen bezeichnen und wenn $\mathfrak{j}$ und $\mathfrak{j}_1$ die zwei diesen Formen zugeordneten Ideale sind, so gilt auch umgekehrt der Satz, daß $\mathfrak{j} \sim \mathfrak{j}_1$ ist.

Hiermit ist aber nun schon von selbst gezeigt, daß der endlichen Anzahl Idealklassen des Körpers $k(\sqrt{m})$ eine endliche Anzahl Klassen quadratischer Formen von der Determinante m entspricht. Die letztere Anzahl ist mindestens gleich, im allgemeinen größer, und zwar im Maximum viermal so groß als die Anzahl der Idealklassen. (S. 196, Probl. 3.)

Einer ambigen Idealklasse entspricht stets eine Formenklasse mit ambigen (zweiseitigen) Formen.

Durch die Übertragung des Minkowskischen Satzes über die praktische Bestimmung der Klassenanzahl h für Idealklassen auf quadratische Formen würde man erhalten: In jeder Formenklasse der Determinante $D = m$ gibt es mindestens eine quadratische Form, deren mittlerer Koeffizient b und deren äußere Koeffizienten a, c die Bedingungen erfüllen: $|b| \leqq |\sqrt{m}|$, $|a| \leqq 2|\sqrt{m}|$ und $|a| \geqq |c|$.

Gauß hat für solche durch ähnliche Ungleichungen beschränkte Formen die Bezeichnung *reduzierte Formen* gebraucht. (S. 196, Probl. 4.)

Die Einheiten eines Zahlkörpers spielen für die quadratischen Formen eine besonders wichtige Rolle: sie liefern alle eigentlichen und uneigentlichen Transformationen einer Form in sich und ferner alle Transformationen einer Form f in eine äquivalente f_1, wenn man *eine* Transformation kennt, welche f in f_1 überführt. Man braucht, um dies einzusehen, nur an die Bildung einer Form f als Norm eines Ausdrucks $ax + (b + \sqrt{m})y$ sich zu erinnern, und diesen Ausdruck mit ε^t zu multiplizieren, dann erhält man die gesuchten Transformationsformeln. (S. 196, Probl. 2.)

Die Darstellung einer Zahl durch eine Form geht der Zerlegung der Zahl im Körper parallel.

Auf die weitere Verfolgung der Analogien zwischen Idealtheorie und Körpertheorie können wir nun verzichten. Es ist klar, daß alle Begriffe, wie: die Multiplikation der Klassen, Einteilung der Klassen in Geschlechter, Charakterensystem eines Geschlechtes usw., sich übertragen lassen.

Zu der Komposition der uneigentlich primitiven Klassen mit Determinanten, welche der Bedingung $D \equiv 1, (4)$ genügen, möge nur noch bemerkt werden, daß man zunächst die Koeffizienten durch 2 dividiert, dann die Komposition ausführt und schließlich die so erhaltene Form doppelt nimmt.

38. Geometrische Darstellung der Ideale.

Es ist bemerkenswert, daß die Theorie des quadratischen Zahlkörpers, welche wir in rein arithmetischer Weise entwickelt haben, auch geometrisch interessante Resultate enthält. In der Tat kann man nämlich die Ideale des Körpers durch geometrische Gebilde deuten, deren Studium nicht bloß für die reine Mathematik, sondern auch für die Mineralogie, spez. für die Kristallographie wichtig und unbedingt notwendig ist. Da die geometrische Betrachtung der bisher gewonnenen Resultate schon an sich sehr reizvoll ist und zugleich manche der bisherigen Ergebnisse von einer neuen Seite zeigt, in gewissem Sinne sogar die eingehende Behandlung des quadratischen Körpers (der ja nur ein Spezialfall einer sehr viel allgemeineren Theorie ist) rechtfertigt, so soll in diesem Paragraphen die geometrische Theorie in ihren Grundzügen auseinandergesetzt werden. Mancher, der gewohnt ist geometrisch zu denken, wird vielleicht durch diese neue Auffassung für die arithmetischen Resultate und Methoden inter-

essiert werden, abgesehen davon, daß die Verfolgung von Analogien immer ein fruchtbares Prinzip der wissenschaftlichen Untersuchung bildet.

Bei den arithmetischen Beweisen hat sich immer wieder ein ganz fundamentaler Unterschied in der Behandlung imaginärer und reeller Körper gezeigt, und diese Verschiedenartigkeit der beiden Arten von Körpern tritt schon in den grundlegenden geometrischen Definitionen sehr stark hervor. Wir behandeln daher die beiden Arten von Zahlkörpern getrennt, zuerst die imaginären und dann die reellen Körper.

Um das volle geometrische Bild zu erhalten, darf der Leser nicht versäumen sich selbst Figuren zu entwerfen. Auch wir halten uns hier zunächst an ein bestimmtes numerisches Beispiel, das aber typisch ist für alle imaginären Körper mit einer Grundzahl $m \not\equiv 1, (4)$.

Wir betrachten den oft behandelten Körper $k(\sqrt{-5})$ mit der Klassenanzahl $h = 2$. Unter Benutzung der Gaußschen Darstellung der komplexen Größen stelle man die ganzen Zahlen des Körpers $a + b\sqrt{-5}$ durch Punkte der Ebene dar, deren Abszissen und Ordinaten in bezug auf ein fest gewähltes rechtwinkliges Koordinatensystem die Zahlen a und $b\sqrt{5}$ sind. Falls man auf der reellen (oder Abszissen-) Achse die Strecke 1 und auf der imaginären (oder Ordinaten-) Achse die Strecke $\sqrt{5}$ als Längeneinheit wählt, sind die ganzen Zahlen des Körpers durch die Punkte mit ganzzahligen rationalen Koordinaten, oder wie man kurz sagen kann, durch die „ganzzahligen" Punkte dargestellt.[1] Die Figur (s. Fig. 1), welche durch die Gesamtheit dieser *Punkte* (ohne die Verbindungslinien zwischen denselben) gebildet wird, heißt ein regelmäßiges **Punktgitter**[2]) und irgend ein spezieller Punkt ein *Gitterpunkt*. Wenn man außer den Punkten die Figur irgend eines doppelten Systems von Parallelen in Betracht

1) Entsprechend einer früheren Festsetzung über die Zahlen des Körpers schließen wir den unendlich fernen Punkt der komplexen Ebene von der Betrachtung aus.

2) Auf diese geometrische Darstellung hat zuerst Gauß aufmerksam gemacht: Ges. Werke II p. 194 (Besprech. eines Werkes von Seeber über ternäre quadratische Formen). Ferner vgl. Lejeune-Dirichlet: Ges. Werke Bd. II p. 21 und ausführlich p. 29. Eingehend findet man die Beziehungen der Zahlentheorie zur Geometrie, speziell zur Theorie der linearen Transformationen, zur Kristallographie, Funktionentheorie und zur Theorie der elliptischen Funktionen studiert von F. Klein: Ausgew. Kapitel der Zahlentheorie. Autogr. Vorlesungen. Gött. 1896 und 1897. 2 Bde.

zieht, welche die Gitterpunkte streifenweise derart verbinden, daß jeder Gitterpunkt der Schnittpunkt zweier bestimmter Geraden des Systems ist und je zwei benachbarte Parallelen konstanten Abstand haben, so bezeichnet man ein solches System als **Parallelgitter.** In dem Beispiel oben bilden unter anderen die Parallelen zu den Achsen in Abständen 1 bzw. $\sqrt{5}$ ein rechtwinkliges Parallelgitter.

Es wird sich im folgenden nur um Punktgitter und Parallelgitter handeln, und es kann daher für die letzteren der Kürze wegen einfach der Name Gitter gebraucht werden, wo eine Zweideutigkeit ausgeschlossen ist.

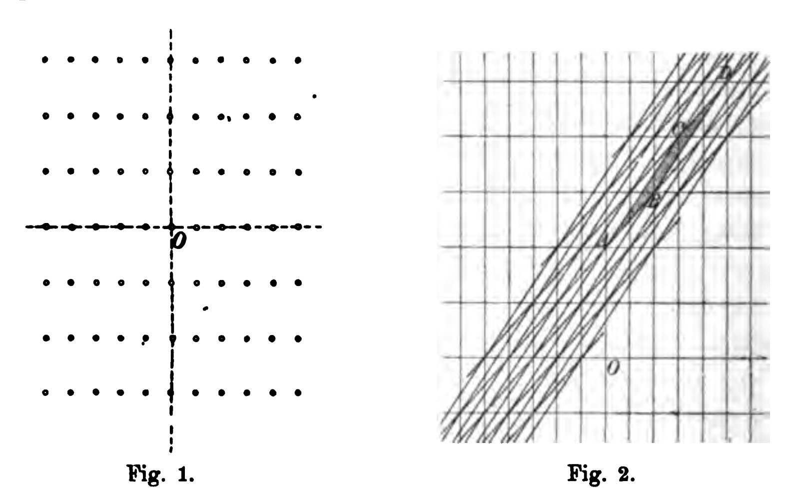


Fig. 1. Fig. 2.

Durch ein Parallelgitter ist die Ebene in unendlich viele Parallelogramme eingeteilt. Ein Parallelogramm, das *keinen* Gitterpunkt in seinem Innern enthält, stellt ein *Elementarparallelogramm* des Gitters dar und kann als **Masche** bezeichnet werden. Die Maschen überdecken die Ebene lückenlos. Ein Gitter ist durch Lage und Dimensionen *einer* Masche vollkommen bestimmt. Zunächst gilt nun die folgende Tatsache.

Satz. *In das Punktgitter ganzzahliger Punkte können unendlich viele verschiedene Parallelgitter eingelagert werden.*

Beweis. (Vergl. Fig. 2.) Man geht zunächst von irgend einem Gitterpunkt A aus, und wählt nun zwei andere Gitterpunkte B und C derart, daß auf den Seiten und innerhalb des Dreiecks ABC kein weiterer Gitterpunkt liegt. Dies kann auf unendlich viele verschiedene Weisen geschehen, wie man leicht einsieht. Hat man B so gewählt, daß innerhalb der Strecke $\overline{AB}$ kein weiterer Gitterpunkt liegt, so

liegen auf der Verbindungslinie AB unendlich viele weitere Punkte, von denen irgend zwei benachbarte einen Abstand gleich $\overline{AB}$ haben, gleichzeitig teilt die Gerade AB alle Gitterpunkte in zwei Hälften rechts und links von AB. Durch eine leichte geometrische Überlegung erkennt man, daß die sämtlichen Gitterpunkte sich auf Parallelen in gleichen Abständen zu der Verbindungslinie AB anordnen lassen, derart, daß auf jeder Parallelen unendlich viele Gitterpunkte in Abständen gleich $\overline{AB}$ liegen. Auf einer der beiden zu AB benachbarten Parallelen, rechts oder links von AB, wählt man irgend zwei aufeinander folgende Gitterpunkte C und D, dann ist wegen $\overline{AB} = \overline{CD}$ das Viereck $ABCD$ ein Parallelogramm, welches nach seiner Konstruktion außer den Eckpunkten keinen Gitterpunkt auf den Seiten oder im Innern enthält. Verschiebt man nun das Parallelogramm so, daß die Seite $\overline{AB}$ in sich verschoben wird und läßt zuerst A nach B, B aber nach E, dann A nach E usw., ferner rückwärts B nach A, A nach F, dann wieder B nach F usw. rücken, so nehmen einerseits die Punkte A und B auf AB und andererseits C, D auf CD der Reihe nach die Lagen aller Gitterpunkte auf den Parallelen AB und CD an. Man erhält einen Parallelstreifen, der durch Querlinien in Maschen geteilt ist. Verschiebt man diesen Streifen in der Richtung dieser Querlinien, also in der Weise, daß A nach C, B nach D oder umgekehrt gebracht wird usw., so wird die Ebene mit lauter Parallelogrammen lückenlos überdeckt und die Ecken A, B, C, D gehen immer wieder in Gitterpunkte über. Man sieht leicht ein, daß bei diesen Verschiebungen das Parallelogramm $ABCD$ immer parallel den Richtungen der ursprünglichen Koordinatenachsen um *ganzzahlige* Strecken an andere Stellen verschoben wurde. Keines der unendlich vielen Parallelogramme kann einen Gitterpunkt im Innern oder auf den Seiten enthalten. In der Tat, enthielte ein Parallelogramm $A'B'C'D'$ einen Gitterpunkt P' auf den Seiten oder im Innern, so verschiebe man $A'B'C'D'$ parallel nach $ABCD$, dann muß der Punkt P' in einen Punkt P auf den Seiten oder im Innern von $ABCD$ übergehen und P müßte ebenfalls ein Gitterpunkt sein. Da nämlich $ABCD$ und $A'B'C'D'$ nach Konstruktion parallel liegen, kann man $A'B'C'D'$ zuerst in der Richtung der einen, dann der zweiten ursprünglichen Koordinatenachse um *ganzzahlige* Strecken verschieben, um die Ecken und Seiten der Parallelogramme zur Deckung zu bringen, daher müssen P und P' gleichzeitig ganzzahlige oder nichtganzzahlige Koordinaten besitzen. Nach Konstruktion enthält jedoch $ABCD$ keinen Gitterpunkt, also kann auch P' kein Gitterpunkt sein.

Durch Parallelverschiebung der Masche $ABCD$ ergab sich aber ein Parallelgitter, das dem Punktgitter so eingelagert ist, daß durch jeden Gitterpunkt je eine Parallele zu AB bezw. AC hindurchgeht. Weil nun die Wahl von $ABCD$ unendlich vieldeutig ist, so kann man unendlich viele verschiedene Parallelgitter in das Punktgitter einlegen.

An die vorhergehende Ableitung sind noch zwei Bemerkungen anzuschließen.

1. Man würde genau dieselben Parallelgitter erhalten, falls man von irgend einem anderen Gitterpunkt statt A als Anfangspunkt ausgegangen wäre. Es sind alle Punkte des Punktgitters gleichberechtigt, indem dasselbe stets parallel *in sich* so verschoben werden kann, daß ein willkürlich gewählter Punkt in den Anfangspunkt A übergeht.

2. Zu einer bestimmten Masche liefert das entsprechende Parallelgitter einfach wieder sämtliche Punkte des Punktgitters. Man kann die Konstruktion des Parallelgitters betrachten als eine fortgesetzte geometrische Addition mit zwei Vektoren, wie z. B. $\overline{AB}$ und $\overline{AC}$. Es stellt dann der Ausdruck:

$$\overline{AB}x_1 + \overline{AC}y_1$$

für ganzzahlige rationale Werte x_1, y_1 sämtliche Punkte des Punktgitters vor. x_1, y_1 sind so die Koordinaten der Gitterpunkte in bezug auf ein (i. a. schiefwinkliges) Koordinatensystem mit den Achsen AB bezw. AC und den Strecken AB bezw. AC als zugehörigen Längeneinheiten.

Nun sind aber die Gitterpunkte nur die geometrischen Bilder der ganzen Zahlen des Körpers, und das Resultat der geometrischen Analyse ist, arithmetisch formuliert, einfach der früher bewiesene Satz: In jedem Zahlkörper kann man auf unendlich viele verschiedene Weisen ein Zahlenpaar ω_1, ω_2 auswählen, so daß durch den Ausdruck:

$$\omega_1 x_1 + \omega_2 y_1$$

mit ganzzahligen rationalen Werten x_1, y_1 alle ganzen Zahlen des Körpers dargestellt werden. Sind ω_1, ω_2 irgend zwei Basiszahlen des Körpers, so stellen die vier Punkte 0, ω_1, ω_2, $\omega_1 + \omega_2$ die Ecken einer Masche vor, und ω_1, ω_2 ergeben die x_1-, y_1-Achse des Koordinatensystems zugleich mit den diesen Achsen zugehörigen Einheitspunkten resp. Längeneinheiten. Wenn dann ferner ω_1^*, ω_2^* zwei andere von ω_1, ω_2 verschiedene Basiszahlen sind, so besteht (vergl. S. 25) zwischen den beiden Paaren stets eine Beziehung:

$$\left.\begin{aligned} \omega_1^* &= r\omega_1 + s\omega_2, \\ \omega_2^* &= t\omega_1 + u\omega_2, \end{aligned}\right\} \quad \text{(T)}$$

wobei r, s, t, u vier ganze rationale Zahlen sind, für welche:

$$ru - st = \pm 1$$

ist.

Die Punkte (Zahlen) 0, ω_1^*, ω_2^* bestimmen ein neues Koordinatensystem, auf welches die Gitterpunkte durch die Koordinaten x, y bezogen sein sollen.

Da nun die Gleichung gilt:

$$\omega_1^* x + \omega_2^* y = (rx + ty)\omega_1 + (sx + uy)\omega_2,$$

so stellt die Transformation:

$$x_1 = rx + ty, \qquad y_1 = sx + uy$$

den Übergang von dem einen Koordinatensystem x, y zu dem zweiten x_1, y_1 vor. Deutet man aber die Größen x, y, x_1, y_1 als Koordinaten in dem Koordinatensystem mit den Achsen AB bezw. AC, so stellt das System:

$$\left.\begin{aligned} x_1 &= rx + ty \\ y_1 &= sx + uy \\ \text{mit der Nebenbedingung} \quad ru - st &= \pm 1, \end{aligned}\right| \quad \text{(S)}$$

wie aus der projektiven Geometrie bekannt ist, eine *affine* Transformation vor, bei welcher Systeme von parallelen Geraden stets wieder in solche übergehen und das Verhältnis entsprechender Flächen konstant ist. Abgesehen vom Nullpunkt wird jeder Punkt des Punktgitters in einen anderen Gitterpunkt transformiert.

In der Theorie der linearen Transformationen bezeichnet man die Transformation (S) als *kontragredient* zu der Transformation (T), welche den Zusammenhang zwischen den verschiedenen Basiszahlenpaaren darstellt, man hat daher den Satz:

Die Transformation (S) *vermittelt analytisch den Übergang von dem Parallelgitter* ω_1, ω_2 *zum anderen* ω_1^*, ω_2^*. Nun lassen sich zwei aufeinanderfolgende lineare Transformationen immer zu einer einzigen Transformation zusammenfassen, deren Determinante gleich dem Produkt der Determinanten der einzelnen Transformationen ist. *Analytisch heißt dies, jedes Parallelgitter läßt sich aus dem rechtwinkligen, oder jedem anderen Gitter durch eine affine Transformation mit der Determinante* ± 1 *ableiten.*

Man beweist sehr leicht mit Hilfe des Produktsatzes für Deter-

minanten, daß der Inhalt eines jeden Elementarparallelogramms, das ein Parallelgitter bestimmt, oder der Inhalt jeder Masche gleich $\sqrt{5}$, also für alle Parallelgitter konstant ist.

Wenn der analytische Übergang von einem Parallelgitter zu einem anderen durch eine affine Transformation mit der Determinante $+1$ oder -1 geschieht, so leiten sich die Parallelgitter geometrisch auseinander ab durch eine einfache Kollineation bezw. Affinität. Die beiden Fälle, daß die Determinante $+1$ oder -1 ist, sind geometrisch durch eine Spiegelung an einer der Achsen aufeinander zurückführbar.

Ich fasse die bisherigen Ergebnisse nochmals zusammen:

Den ganzen Zahlen eines quadratischen Zahlkörpers entsprechen die Punkte eines Punktgitters. In dieses Punktgitter lassen sich unendlich viele Parallelgitter mit Maschen von gleichem Flächeninhalte einlagern. Jedes Parallelgitter ist einer bestimmten Basis des Körpers zugeordnet. Irgend zwei Parallelgitter sind analytisch miteinander durch eine affine Transformation mit der Determinante ± 1 *verbunden, und diese Transformation ist kontragredient zu derjenigen, welche die zugehörigen Paare von Basiszahlen verbindet.*

Der Satz: „Das Produkt, die Summe, die Differenz von irgend zwei ganzen Zahlen eines Zahlkörpers ist stets wieder eine ganze Zahl des Körpers“ lautet für das zugehörige Punktgitter etwa:

1. Das Produkt von irgend zwei Gitterpunkten ist wieder ein Gitterpunkt.

2. Die $\begin{matrix}\text{Summe}\\ \text{Differenz}\end{matrix}$ von zwei Gitterpunkten ist stets wieder ein Gitterpunkt.

Bei dieser Formulierung steht eben das Wort Gitterpunkt anstatt der komplexen Zahl, welche dem Gitterpunkt zugehört, und unter Multiplikation, Addition und Subtraktion der Gitterpunkte ist die geometrische Darstellung dieser Operationen in der Gaußschen Ebene zu verstehen.

Ist jetzt α eine ganze Zahl des Körpers, so besteht das Hauptideal (α) aus der Gesamtheit aller ganzen Zahlen des Körpers, welche durch α teilbar sind.

Demgemäß stellen wir das Hauptideal (α) geometrisch dar durch die Gesamtheit aller derjenigen Gitterpunkte in der Ebene, welche durch den Gitterpunkt α teilbar sind, oder, wie man auch sagen kann, durch die Gesamtheit aller Gitterpunkte, die aus den Gitterpunkten des Körpers durch Multiplikation mit α hervorgehen. Es ist zu

zeigen, daß diese Punkte ebenfalls ein Punktgitter bilden. Bezeichnet man ein Gitter, das zum Körper gehört, kurz als *Grundgitter*, so kann man alsdann sagen, daß dem Hauptideal (α) ein *Gitter* (α) entspricht. [Vgl. hierzu und zum folgenden Fig. 3, wo das Ideal $(\alpha) = (1 + \sqrt{-5})$ dargestellt ist.]

Multipliziert man die Punkte des Grundgitters, welche auf einer Geraden liegen, mit α, so erhält man Punkte, welche alle wieder auf einer Geraden liegen.

Es sei nämlich $\alpha = \bar{a} e^{i\hat{a}}$, und $\varkappa = r e^{i\varphi}$ (wo $i = \sqrt{-1}$ ist) ein beliebiger Punkt, dann erfüllen die Polarkoordinaten r, φ derjenigen Punkte $\varkappa$, welche auf einer Geraden liegen, die Gleichung:

$$r \cos(\delta - \varphi) = d,$$

wo δ, d Neigung und Länge des Lotes vom Nullpunkte auf die Gerade bezeichnen.

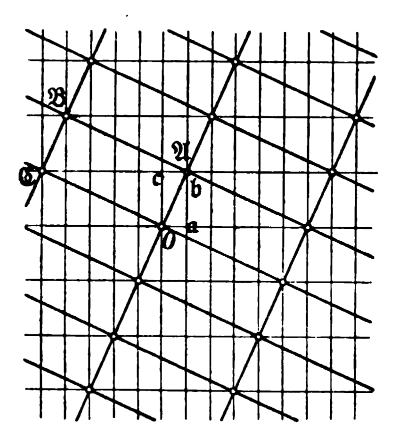


Fig. 3.

Aus den Punkten der Geraden gehen durch Multiplikation mit α die Punkte $\varkappa_1 = Re^{i\Phi} = \bar{a} r e^{i(\hat{a}+\varphi)}$ $(i = \sqrt{-1})$ hervor. Setzt man nun:

$$\delta_1 = \delta + \alpha, \qquad d_1 = d\bar{a},$$

so erfüllen die Werte R, Φ die Gleichung:

$$R \cos(\delta_1 - \Phi) = d_1,$$

d. h. es liegen auch alle Punkte $\varkappa_1$ wieder auf einer Geraden, weil δ_1, d_1 Konstante sind. Ferner geht aus der letzten Gleichung noch hervor, daß parallelen Geraden, mit demselben Wert δ, wieder parallele Gerade mit demselben Wert δ_1 entsprechen. Aus der Form $\varkappa_1 = \bar{a} r e^{\sqrt{-1}\,(\hat{a}+\varphi)}$ folgt, daß bei der Multiplikation mit α ein vom Nullpunkt aus-

gehender Vektor um den Winkel $\widehat{\alpha}$ gedreht und im Verhältnis $\bar{a}r:r$ gestreckt wird. Jede Figur geht daher in eine ähnliche Figur über.

Da nun das Ideal (α) aus (1) durch Multiplikation mit α hervorgeht, so stellt also (α) auch ein dem Grundgitter ähnliches Gitter vor.

Einer Masche des Grundgitters mit den Ecken 0, 1, $1 + \sqrt{-5}$, $\sqrt{-5}$ z. B. entspricht im Gitter (α) ein Rechteck mit den Ecken $0 . \alpha$, α, $(1 + \sqrt{-5})\alpha$, $\sqrt{-5} . \alpha$. Dieses Rechteck ist der Masche des rechtwinkligen Grundgitters ähnlich, es kann keinen weiteren Gitterpunkt des Gitters (α) enthalten. Man hat daher den Satz:

Satz. *Jedem Hauptideal* (α) *zu der Zahl* $\alpha = \bar{a} e^{\sqrt{-1}\,\hat{\alpha}}$ *entspricht ein Punktgitter, das dem Grundgitter ähnlich ist und aus diesem durch eine Drehung um den Winkel* $\widehat{\alpha}$ *und eine Dehnung im Verhältnis* $\bar{a}:1$ *hervorgeht.*

Insbesondere folgt aus den bisherigen Betrachtungen:

Allen Hauptidealen entsprechen ähnliche Punktgitter. Dem Ideal (1) entspricht das Grundgitter selbst.

Analytisch bedeutet die Ableitung des Gitters (α) aus dem Grundgitter eben nur die Anwendung einer affinen Transformation auf das letztere.

Setzt man $\alpha = a + b\sqrt{-5}$, und bezeichnet die Punkte des Grundgitters und des Gitters (α) mit $x + y\sqrt{-5}$ bezw. $X + Y\sqrt{-5}$, so ist:

$$\begin{cases} X = ax - 5by \\ Y = bx + ay, \end{cases}$$

d. h. eben, das Punktgitter (α) ist mit dem Grundgitter durch eine Transformation mit der Determinante $a^2 + 5b^2 = \bar{a}^2$ verbunden. Dem Punktgitter (α) kann man wieder unendlich viele Parallelgitter einlagern, welche untereinander durch affine Transformationen mit der Determinante ± 1 zusammenhängen, genau so wie dies für die Parallelgitter zum Grundgitter bewiesen wurde.

Es läßt sich jeder Basis des Ideals (α), z. B zu α, $\alpha\sqrt{-5}$, usw. ein Parallelgitter zuordnen, dessen Elementarparallelogramm die Punkte 0, α, $\alpha\sqrt{-5}$, $\alpha + \alpha\sqrt{-5}$ zu Ecken hat. Verschiedenen Basiszahlen entsprechen die verschiedenen Parallelgitter, und man leitet aus dem Zusammenhang der ersteren die affine Transformation zwischen den letzteren ab. Man kann daher wieder folgenden Satz aufstellen:

Satz. *Einem Ideal* (α) *ist stets ein bestimmtes dem Grundgitter ähnliches Punktgitter zugeordnet. Diesem Punktgitter lassen sich unendlich viele Parallelgitter einlagern, indem jede Basis des Ideals ein*

solches Parallelgitter definiert. Irgend zwei der Parallelgitter hängen durch eine affine Transformation mit der Determinante ± 1 *miteinander zusammen und diese Transformation ist kontragredient zu derjenigen Transformation, welche die den zwei Parallelgittern entsprechenden Paare von Basiszahlen verbindet. Alle Parallelgitter haben inhaltsgleiche Maschen.*

[Anmerkung. Bei der Aufstellung der affinen Transformation, durch welche ein Parallelgitter (α) in ein anderes übergeführt wird, legt man zweckmäßig ein schiefwinkliges Koordinatensystem zugrunde, dessen Achsen mit den Richtungen der zwei Parallelscharen eines der beiden Parallelgitter selbst zusammenfallen. Man könnte natürlich die Transformationsformeln auch in bezug auf das ursprüngliche rechtwinklige Koordinatensystem aufstellen. Dabei erhält man aber, wovon der Leser sich selbst überzeugen mag, Transformationsformeln mit rationalen, aber nicht mehr notwendig ganzzahligen Koeffizienten und der Determinante ± 1.

Die Aufstellung dieser Formeln ist indessen ohne Bedeutung, da eben über die Wahl eines Koordinatensystems und über die Wahl der Längeneinheiten auf den Achsen nur der spezielle Zweck entscheidet.]

Jede Masche eines Gitters enthält außer den 4 Eckpunkten noch eine Anzahl Gitterpunkte des *Grundgitters*, im Innern oder auf den Seiten. Wir wollen festsetzen, daß zu den Punkten einer Masche gerechnet werden sollen: 1. ein Eckpunkt der Masche (so daß also jeder Eckpunkt nur zu einer einzigen Masche gehört), 2. die Punkte, welche, abgesehen von den Ecken, auf den beiden in dem Eckpunkt zusammenstoßenden Maschenseiten liegen, 3. die Punkte im Innern der Masche. Nach dieser Festsetzung soll nun die Anzahl der Punkte des Grundgitters, die in einer Masche des Gitters (α) liegen, bestimmt werden.

Zunächst erkennt man, daß alle Maschen eines und desselben Gitters gleich viele Punkte des Grundgitters enthalten. Da ferner zwei Maschen von zwei verschiedenen Gittern durch eine affine Transformation ineinander übergehen, welche das Innere einer Masche in das Innere der anderen überführt, so folgt, daß auch irgend zwei Maschen zweier verschiedener Parallelgitter gleich viele ganzzahlige Punkte enthalten. Man darf also für die Bestimmung der gesuchten Anzahl irgend eine geeignete Masche auswählen. Es empfiehlt sich, diejenige Masche zu nehmen, welche zur Normalbasis des Ideals gehört.

Sei $\alpha = a + b\sqrt{-5}$, und es besitzen a und b den größten gemein-

samen Teiler t, so ist die Normalbasis $\frac{a^2+5b^2}{t}$, $a_1 + t\sqrt{-5}$, wobei a_1 ein Vielfaches von t ist. Die Masche ist nun so gelegen, daß eine Seite in die x-Achse des Koordinatensystems fällt, diese Seite enthält $\frac{a^2+5b^2}{t}$ Punkte des Grundgitters, während auf der durch $a_1 + t\sqrt{-5}$ bestimmten Seite eben t solcher Punkte liegen, und es enthält also die Masche insgesamt $n(\alpha) = a^2 + 5b^2$ Punkte des Grundgitters; in der Tat bilden diese Punkte mod (α) ein vollständiges System inkongruenter Zahlen.

Satz. *Wenn man dem Punktgitter* (α) *ein Parallelgitter einlagert, so enthält jede Masche* $n(\alpha)$ *Gitterpunkte des Grundgitters, und diese Gitterpunkte gehören zu einem vollständigen System mod* (α) *inkongruenter Zahlen des Körpers.*

Die Darstellung eines Hauptideals hat sich schon in einer solchen Weise ausführen lassen, daß wir uns im folgenden umso kürzer fassen können.

Einem beliebigen Nichthauptideal:

$$\mathfrak{j} = (\alpha, \beta, \gamma, \ldots \lambda_1\alpha + \lambda_2\beta + \lambda_3\gamma, \ldots)$$

sei jetzt das Punktgitter aller Punkte $\alpha, \beta, \ldots$ zugeordnet. Da man das Ideal $\mathfrak{j}$ durch eine Basis ι_1, ι_2 in der Weise darstellen kann daß:

$$\mathfrak{j} = (\iota_1, \iota_2, x\iota_1 + y\iota_2)$$

ist, wo x, y alle ganzen rationalen Zahlen von $-\infty$ bis $+\infty$ durchlaufen, so folgt, daß man dem Punktgitter $\mathfrak{j}$ ein Parallelgitter einlagern kann mit der Masche, deren Ecken die Punkte 0, ι_1, ι_2, $\iota_1 + \iota_2$ sind. Jeder anderen Basis, die man im Ideal $\mathfrak{j}$ auswählen kann, entspricht ein dem Punktgitter eingelagertes Parallelgitter, und diese Parallelgitter hängen durch affine Transformationen miteinander zusammen, wobei die Inhalte zugeordneter Maschen gleich sind.

Die Anzahl der Punkte des Grundgitters, welche in einer Masche eines solchen Parallelgitters enthalten sind, ist gleich der Norm des Ideals $|n(\mathfrak{j})|$, und es bilden die zu diesen Gitterpunkten gehörigen Zahlen mod $(\mathfrak{j})$ ein vollständiges System inkongruenter Zahlen des Körpers.

Es seien nun $\mathfrak{j}$ und $\mathfrak{j}_1$ zwei Nichthauptideale aus der gleichen Idealklasse, dann soll die Beziehung zwischen den beiden zugehörigen Punktgittern aufgestellt werden.

Nach der Definition der Äquivalenz gibt es zwei ganze Zahlen des Körpers, so daß $\frac{\mathfrak{j}}{\mathfrak{j}_1} = \frac{\alpha_1}{\alpha}$ oder $(\alpha)\mathfrak{j} = (\alpha_1)\mathfrak{j}_1$ ist. Das Produkt $(\alpha)\mathfrak{j}$ ist

aber das Ideal, das aus $\mathfrak{j}$ hervorgeht, wenn man alle Zahlen des Ideals mit α multipliziert. Schreibt man wieder $\alpha = \bar{a} e^{\sqrt{-1}\hat{\alpha}}$, so besteht diese Multiplikation für die Gitterpunkte von $\mathfrak{j}$ darin, daß jeder Vektor um den Winkel $\hat{\alpha}$ gedreht und im Verhältnis $\bar{a}:1$ verlängert wird. Dadurch geht aus dem Punktgitter (oder Gitter) $\mathfrak{j}$ ein neues Punktgitter (Gitter) $(\alpha)\mathfrak{j}$ hervor, das zu dem ersten ähnlich ist, aus diesem selbst durch eine Drehung um $\hat{\alpha}$ und Vergrößerung im Verhältnis $\bar{a}:1$ abzuleiten ist. D. h. jedem Gitter, das dem Punktgitter $\mathfrak{j}$ eingelagert ist, entspricht ein ähnliches Gitter des Punktgitters $(\alpha)\mathfrak{j}$. Ebenso geht das Punktgitter $(\alpha_1)\mathfrak{j}_1$ aus dem Gitter $\mathfrak{j}_1$ durch eine Drehung und Ähnlichkeitstransformation hervor, somit sind auch die Punktgitter $\mathfrak{j}$ und $\mathfrak{j}_1$ ähnlich zueinander.

Wir können daher den allgemeinen Satz formulieren:

Zwei Ideale aus derselben Idealklasse lassen sich durch ähnliche Punktgitter geometrisch darstellen. Zwei diesen Punktgittern eingelagerte Parallelgitter hängen miteinander durch eine affine Transformation mit der Determinante $\pm\sqrt{n\left(\frac{\mathfrak{j}_1}{\mathfrak{j}}\right)}$ *zusammen.*

Äquivalenz zweier Ideale ist Ähnlichkeit der zugehörigen Punktgitter oder der in diese eingelagerten Parallelgitter.

Dem Produkt $\mathfrak{j}\mathfrak{j}_1$ zweier Ideale entspricht wieder ein Ideal, das man nun als die geometrische Komposition der beiden Punktgitter $\mathfrak{j}$ und $\mathfrak{j}_1$ betrachten muß. Dieses Punktgitter $\mathfrak{j}\mathfrak{j}_1$ enthält alle Gitterpunkte, welche den Punktgittern $\mathfrak{j}$ und $\mathfrak{j}_1$ gemeinsam sind.

Faßt man alle Zahlen der beiden Ideale $\mathfrak{j}$ und $\mathfrak{j}_1$ zu einem neuen Ideal $\mathfrak{J}$ zusammen, so ist $\mathfrak{J}$ der größte gemeinsame Idealteiler der Ideale $\mathfrak{j}$ und $\mathfrak{j}_1$ und ergibt sich geometrisch durch Übereinanderlagerung der Punktgitter $\mathfrak{j}$ und $\mathfrak{j}_1$.

Die bis jetzt aufgestellten Sätze gelten ohne weiteres für alle Körper $k(\sqrt{m})$, für welche $m \not\equiv 1, 4$ ist. Falls $m \equiv 1, (4)$ ist, sind die ganzen Zahlen des Körpers: $a + b\,\frac{1+\sqrt{m}}{2}$. Die Gitterpunkte des Grundgitters bestehen jetzt aus den ganzzahligen Punkten eines schiefwinkligen Koordinatensystems, das so gewählt werden kann, daß sein Nullpunkt in den Punkt 0 und die Einheitspunkte auf den Koordinatenachsen in die Punkte 1 resp. $\frac{1+\sqrt{m}}{2}$ gelegt sind.

Unter den Parallelgittern, welche dem Punktgitter der ganzen Zahlen des Körpers eingelagert werden können, befindet sich keines

mit rechteckigen Maschen. Man kann als Maschen eines Gitters Rhomben wählen, wenn man den Rhombus mit den Ecken:

$$0, \frac{1+\sqrt{m}}{2}, \quad 1, \frac{1-\sqrt{m}}{2},$$

als Masche annimmt. Für das Punktgitter des Körpers $k(\sqrt{-3})$ haben die von ± 1 verschiedenen Einheiten eine besondere Bedeutung, sie definieren die Symmetrieeigenschaften des Punktgitters, wie dies später bei den reellen Körpern gezeigt werden soll. Im übrigen können die oben aufgeführten Sätze für den jetzigen Fall $m \equiv 1$, (4) wörtlich übertragen werden.

Den arithmetischen Satz von der Endlichkeit der Klassenanzahl h des Körpers $k(\sqrt{m})$ kann man nunmehr in geometrischer Form so aussprechen:

Satz.[1]) *Die unendlich vielen Punktgitter, welche man aus dem Punktgitter der ganzen Zahlen des Körpers $k(\sqrt{m})$ herausgreifen kann, indem man Untergruppen aus dem letzteren zu Punktgittern vereinigt, verteilen sich auf h Gruppen (Klassen) so, daß alle Punktgitter einer und derselben Gruppe (Klasse), mit den eingelagerten Parallelgittern, untereinander ähnlich sind.*

Die Gitter, die einer und derselben Klasse angehören, und nur diese, gehen durch Ähnlichkeitstransformationen ineinander über.

Nachdem oben darauf hingewiesen ist, daß alle Parallelgitter, welche einem und demselben Punktgitter eingelagert sind, Maschen mit gleichem Inhalt besitzen, kann man kurzweg von dem *Mascheninhalt* des Punktgitters sprechen. Durch eine direkte Berechnung findet man als Mascheninhalt für das zum Ideal $\mathfrak{j}$ gehörige Punktgitter $\frac{1}{2} n(\mathfrak{j}) \sqrt{|d|}$, wenn $|d|$ die positiv genommene Diskriminante des Körpers bedeutet. Alsdann läßt sich der Satz von Minkowski folgendermaßen formulieren:

Satz. *In jeder der h Gruppen ähnlicher Punktgitter des Körpers $k(\sqrt{m})$ befindet sich immer mindestens eines mit einem Mascheninhalt, der kleiner ist als $\frac{|d|}{2}$.*

Dieser Satz enthält also ein Mittel zur geometrischen Konstruktion der Punktgitter.

Vom geometrischen Gesichtspunkt aus hätte es noch ein großes Interesse, eine Frage zu erörtern, welche in noch unbestimmter Fassung

1) Vgl. F. Klein, l. c. Bd. II, S. 94 ff.

so formuliert werden kann: Zu einem gegebenen Punktgitter das möglichst einfache Parallelgitter zu konstruieren.

Ein Punktgitter repräsentiert für uns i. a. ein Ideal, und die Frage wäre arithmetisch: die einfachste Basis des Ideals zu bestimmen. Bezeichnet man, was nahe liegt, die Normalbasis als einfachste Basis des Körpers, so kann man daraus folgenden geometrischen Satz ableiten: In jedes Punktgitter, dessen Mascheninhalt $< \frac{|d|}{2}$ ist, kann man stets ein Elementarparallelogramm einlegen, dessen Seiten $< \sqrt{|d|}$ resp. $\sqrt{\frac{|d|}{2}}$ sind.

Die einfachen geometrischen Deutungen, welche für die Begriffe und Sätze des imaginären Zahlkörpers sich aufstellen lassen, sind wesentlich geknüpft an die geometrische Darstellung der komplexen Größen und an die einfache Art, wie die Grundoperationen mit komplexen Größen sich geometrisch ausführen lassen. Bekanntlich beruht diese Einfachheit darauf, daß man jede komplexe Zahl $a + \sqrt{-1}\, b$ auf die Form $re^{\sqrt{-1}\varphi} = r(\cos\varphi + \sqrt{-1}\sin\varphi)$ bringen kann, und daß daher die Multiplikation von zwei komplexen Zahlen auf die Multiplikation der reellen absoluten Beträge oder Radienvektoren r, r_1 und die Addition der Neigungen φ, φ_1 hinauskommt.

Für einen reellen Körper $k(\sqrt{m})$ [wobei zunächst wieder $m \not\equiv 1, (4)$ sei] kann man in analoger Weise ein Gitter der ganzen Zahlen konstruieren. Man legt hierzu ein rechtwinkliges Koordinatensystem zugrunde, auf dessen x-Achse die Länge 1, auf dessen y-Achse die Länge $\sqrt{m}$ als Längeneinheiten gewählt sind und stellt jede Zahl des Körpers $a + b\sqrt{m}$ durch einen Punkt mit den Koordinaten (a, b) dar. Dann gilt zwar der Satz: Gitterpunkt $\pm$ Gitterpunkt gleich Gitterpunkt; aber die Multiplikation zweier Gitterpunkte ist überhaupt nicht definiert. Wenn man ferner irgend ein Ideal, wie es früher geschah, durch ein Gitter darstellt, so kann im elementaren Sinn von einer Ähnlichkeit der Gitter aller Hauptideale oder aller Ideale einer Klasse nicht mehr die Rede sein.

Um für die reellen Körper die geometrischen Deutungen und die daraus sich ergebenden Resultate in Übereinstimmung zu bringen mit den Sätzen für den imaginären Körper, benützen wir einen Gedanken, den Herr Klein[1]) wohl zuerst zur Betrachtung der Punktgitter benützt hat: wir setzen an die Stelle der elementaren Maß-

1) F. Klein, l. c., S. 50 ff. und spez. 71.

bestimmung für Strecken und Winkel, welche die Euklidische Maßbestimmung heißt, eine andere passend definierte *pseudometrische* Maßbestimmung.

Es handelt sich dabei um Definitionen, die sozusagen in die elementare Geometrie eingelegt sind, damit man ein geometrisches System ohne Widersprüche erhält.

Wir betrachten das Punktgitter der ganzen Zahlen des Körpers $k(\sqrt{m})$, dessen Konstruktion oben schon angegeben wurde. Den Betrachtungen liegt also ein gewöhnliches rechtwinkliges Koordinatensystem zugrunde, mit dem Ursprung 0 und den Einheiten 1 und $\sqrt{m}$ für die Achsen. Nun definieren wir für dieses System: 1.) die Entfernung zweier Punkte, 2.) den Winkel zweier Geraden, 3.) den Inhalt einer endlichen geschlossenen Figur.

1.) Sei x, $y\sqrt{m}$ oder (x, y) ein Punkt P des Punktgitters und O der Punkt $(0, 0)$, so definiere die Gleichung:

$$r = +\sqrt{x^2 - my^2}$$

die Entfernung $\overline{OP}$.

Alle Punkte, welche von O die Entfernung $r = 1$ haben, erfüllen daher die Gleichung:

$$1 = x^2 - my^2,$$

sie liegen auf einer reellen Hyperbel, deren reelle Achse in der x-Achse liegt und die Länge 2 hat. Diese Hyperbel heißt die *Eichkurve* für die Maßbestimmung. Auf jeder Geraden durch den Ursprung O definiert sie nämlich eine (besondere) Längeneinheit, die dann für die ganze Erstreckung dieser Nullpunktsgeraden die Streckeneinheit (die Maßzahl) darstellt. Die Hyperbel entspricht dem Kreis $x^2 + y^2 = 1$ der elementaren Maßbestimmung. Alle Punkte, welche auf einer von den zwei Asymptoten der Hyperbel:

$$x - \sqrt{m}y = 0, \quad x + \sqrt{m}y = 0$$

liegen, haben vom Nullpunkt die Entfernung 0, denn für irgend einen Punkt dieser Asymptoten ist $r = \sqrt{x^2 - my^2} = 0$. Die Asymptoten nehmen in der neuen Maßbestimmung eine ganz eigenartige Stellung ein, sie entsprechen den Linien $x \pm \sqrt{-1}\,y = 0$ der elementaren Geometrie. Wegen der fundamentalen Eigenschaft, daß irgend zwei Punkte einer Asymptote die Entfernung 0 besitzen, ist auf sie der Name *Minimalgeraden* übertragen worden, der auch für die Geraden:

$$x + \sqrt{-1}\,y = 0, \quad x - \sqrt{-1}\,y = 0$$

in der gewöhnlichen Geometrie gebraucht wird.

Alle Punkte, welche *innerhalb* der Asymptoten liegen, haben *reelle* Entfernungen von 0. Dagegen ist für die Punkte $x,\ y\sqrt{m}$, welche nicht im selben Winkelraum der Asymptoten wie die Hyperbel gelegen sind, $x^2 - my^2$ negativ, also r imaginär. Für diese imaginären Entfernungen von 0 kann man aber doch die reelle Hyperbel

$$x^2 - my^2 = -1$$

als Eichkurve benützen, wenn jeder Maßzahl noch der Faktor $i = \sqrt{-1}$ beigefügt wird.

Seien ferner $x,\ y\sqrt{m}$ und $x_1,\ y_1\sqrt{m}$ zwei beliebige Punkte, so setzen wir für ihre Entfernung r die Gleichung an:

$$r = +\sqrt{(x - x_1)^2 - m(y - y_1)^2}.$$

2.) Um die Neigung des Radius OP gegen die x-Achse zu bestimmen, gebraucht man einen Kunstgriff. Die Kreisfunktionen, die bei den komplexen Größen $a + \sqrt{-1}\,b$ zur Verwendung kommen, werden durch die hyperbolischen Funktionen ersetzt, so wie in der Längenbestimmung die Hyperbel an die Stelle des Kreises getreten ist.

Wir setzen:

$$x + y\sqrt{m} = r(\operatorname{ch}\varphi + \operatorname{sh}\varphi),$$

oder getrennt:

$$\begin{cases} x = r\operatorname{ch}\varphi, \\ y\sqrt{m} = r\operatorname{sh}\varphi, \end{cases}$$

und definieren den so bestimmten Winkel φ als die Neigung des Radius OP gegen die x-Achse.

Der Deutlichkeit wegen mögen die Definitionsgleichungen für die hyperbolischen Funktionen und die fundamentalen Relationen zwischen denselben hier angeführt werden. Es ist:

$$\operatorname{ch}\varphi = \frac{e^{\varphi} + e^{-\varphi}}{2}, \quad \operatorname{sh}\varphi = \frac{e^{\varphi} - e^{-\varphi}}{2};$$

daher gelten die Formeln:

$$\operatorname{ch}(-\varphi) = \operatorname{ch}\varphi, \quad \operatorname{sh}(-\varphi) = -\operatorname{sh}\varphi,$$

$$\operatorname{ch}^2\varphi - \operatorname{sh}^2\varphi = 1, \quad \text{also} \quad x^2 - my^2 = r^2.$$

Ferner ist:

$$\operatorname{ch}\varphi + \operatorname{sh}\varphi = e^{\varphi}, \quad \operatorname{ch}\varphi - \operatorname{sh}\varphi = e^{-\varphi}.$$

Hieraus folgt für die Multiplikation und Division:

$$(\operatorname{ch}\varphi + \operatorname{sh}\varphi)(\operatorname{ch}\varphi_1 + \operatorname{sh}\varphi_1) = \operatorname{ch}(\varphi + \varphi_1) + \operatorname{sh}(\varphi + \varphi_1),$$

$$(\operatorname{ch}\varphi + \operatorname{sh}\varphi)(\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) = \operatorname{ch}(\varphi - \varphi_1) + \operatorname{sh}(\varphi - \varphi_1),$$

$$(\operatorname{ch}\varphi - \operatorname{sh}\varphi)(\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) = \operatorname{ch}(\varphi + \varphi_1) - \operatorname{sh}(\varphi + \varphi_1),$$

und:

$$(\operatorname{ch}\varphi + \operatorname{sh}\varphi) : (\operatorname{ch}\varphi_1 + \operatorname{sh}\varphi_1) = \operatorname{ch}(\varphi - \varphi_1) + \operatorname{sh}(\varphi - \varphi_1),$$
$$(\operatorname{ch}\varphi + \operatorname{sh}\varphi) : (\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) = \operatorname{ch}(\varphi + \varphi_1) + \operatorname{sh}(\varphi + \varphi_1),$$
$$(\operatorname{ch}\varphi - \operatorname{sh}\varphi) : (\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) = \operatorname{ch}(\varphi - \varphi_1) - \operatorname{sh}(\varphi - \varphi_1).$$

Nach diesen Formeln bietet also die Multiplikation zweier Zahlen $x + y\sqrt{m} = r(\operatorname{ch}\varphi + \operatorname{sh}\varphi)$ und $x_1 + y_1\sqrt{m} = r_1(\operatorname{ch}\varphi + \operatorname{sh}\varphi)$ eine vollkommene Analogie dar mit der Multiplikation komplexer Zahlen.

Zur expliziten Bestimmung der Neigung φ des Radius OP hat man die simultanen Gleichungen:

$$x + y\sqrt{m} = re^{\varphi}, \quad x - y\sqrt{m} = re^{-\varphi},$$

oder:

$$e^{2\varphi} = \frac{x + y\sqrt{m}}{x - y\sqrt{m}},$$

daher ist:

$$\varphi = \tfrac{1}{2}\operatorname{Log}\frac{x + y\sqrt{m}}{x - y\sqrt{m}}.$$

Der Ableitung nach, da $e^{2\varphi} = e^{2\varphi + 2k\pi\sqrt{-1}}$ ist, ist φ nur mod $(\pi\sqrt{-1})$ bestimmt. Unter Log soll der (*reelle*) Hauptwert des Logarithmus naturalis des Quotienten $\frac{x + y\sqrt{m}}{x - y\sqrt{m}}$ verstanden werden. Alsdann ist noch eine Unterscheidung zu machen zwischen den Radien OP, die in dem Raum *zwischen* den Asymptoten der Hyperbel $x^2 - my^2 = 1$ verlaufen, und denjenigen Radien, die außerhalb dieser Asymptoten verlaufen, also die Hyperbel nicht schneiden.

Im erstern Fall ist $x^2 - my^2 > 0$, oder die Norm der Zahl $x + y\sqrt{m}$ positiv, also r reell. Dann ist

$$\varphi = \tfrac{1}{2}\operatorname{Log}\frac{x + y\sqrt{m}}{x - y\sqrt{m}} = \tfrac{1}{2}\operatorname{Log}\frac{(x + y\sqrt{m})^2}{n(x - y\sqrt{m})},$$

oder φ ist ein *reeller* Winkel.

Im zweiten Fall ist $x^2 - my^2 < 0$ oder $n(x + y\sqrt{m})$ negativ, dann ist:

$$\varphi = \tfrac{1}{2}\operatorname{Log}\frac{(x + y\sqrt{m})^2}{n(x - y\sqrt{m})} = \tfrac{1}{2}\operatorname{Log}\left[-\frac{(x + y\sqrt{m})^2}{n(x - y\sqrt{m})}\right] + \tfrac{1}{2}\operatorname{Log}(-1),$$

also:

$$\varphi = (\varphi) + \tfrac{1}{2}i\pi.$$

Der Winkel φ ist also eine komplexe Größe, indem nun hier und im folgenden $i = \sqrt{-1}$ gesetzt werden soll.

Als Winkel zweier Radien OP und OP_1 definieren wir die

Differenz der Neigungen $\varphi - \varphi_1$, indem wir dem Winkel ein bestimmtes Vorzeichen $\pm$ beilegen nach einem einmal angenommenen Richtungssinn. Zwei Radien, welche durch eine der beiden Asymptoten getrennt sind, schließen einen *komplexen* Winkel ein, während zwei Radien, die nicht durch eine Asymptote getrennt sind, einen *reellen* Winkel einschließen.

Aus der Formel für φ folgt, daß jede Asymptote: $x \pm y\sqrt{m} = 0$, mit der x-Achse sowohl als mit einem beliebigen Radius OP einen unendlich großen Winkel einschließt.

3.) Die Flächeninhalte definieren wir so, daß wir ein Quadrat mit der Seitenlänge 1 im elementaren Sinn als Flächeneinheit wählen. Die Flächeninhalte berechnen sich also nach der gewöhnlichen Vorschrift der elementaren Geometrie, bezw. der Integralrechnung.

So hat beispielsweise das Parallelogramm mit den Ecken 0, $a + b\sqrt{m}$, $(a + a_1) + (b + b_1)\sqrt{m}$, $a_1 + b_1\sqrt{m}$ den Inhalt:

$$f = \begin{vmatrix} a & b\sqrt{m} \\ a_1 & b_1\sqrt{m} \end{vmatrix} = (ab_1 - a_1 b)\sqrt{m},$$

und insbesondere hat eine Masche in dem Gitter der ganzen Zahlen des Körpers, das auch weiter Grundgitter heißen soll, den Inhalt $\sqrt{m}$.

Nach diesen Festsetzungen ist zunächst klar, daß für die Punkte des Grundgitters wie für die Zahlen des Körpers die Fundamentalsätze über die Grundoperationen der Addition, Subtraktion, Multiplikation und Division gelten. Unter dem Produkt zweier Gitterpunkte ist dabei zu verstehen: Addition der Neigungen der zugehörigen Radien und Multiplikation der zugehörigen Radienvektoren $r \cdot r_1$.

Ein Hauptideal (α) ist natürlich dargestellt durch ein Punktgitter, das aus sämtlichen durch α teilbaren Gitterpunkten des Grundgitters besteht. Die Darstellung des Ideals (α) durch irgend eine Basis, z. B. α, $\alpha\sqrt{m}$:

$$(\alpha) = (\alpha, \alpha\sqrt{m}, \alpha x + \alpha\sqrt{m}\, y),$$

wo x, y reelle ganze rationale Zahlen sind, zeigt, daß dem Gitter wieder unendlich viele Parallelgitter eingeschrieben werden können.

Man erhält das Punktgitter (α), indem man jeden Gitterpunkt des Grundgitters mit α multipliziert. Sei nun $\alpha = a + b\sqrt{m} = \bar{a}e^{\vartheta}$ und $x + y\sqrt{m} = re^{\varphi}$ ein beliebiger Punkt des Gitters, so ergibt sich für das Produkt dieser beiden Punkte:

$$X + Y\sqrt{m} = ax + bmy + (bx + ay)\sqrt{m} = \bar{a}re^{(\hat{a}+\varphi)},$$

und hieraus folgt der Satz:

Jeder Gitterpunkt von (α) *geht aus einem solchen des Grundgitters hervor durch eine Drehung des Radiusvektors des letztern um den Winkel* $\hat{\alpha}$ *und eine Streckung im Verhältnis* $\bar{a}:1$. Oder man kann sagen:

Das Punktgitter (α) hängt mit dem Punktgitter des Körpers durch eine Substitution zusammen:

$$\begin{cases} X = ax + bmy \\ Y = bx + ay \end{cases}$$

mit der Transformationsdeterminante $a^2 - b^2m = \bar{a}^2$.

In dem eben ausgesprochenen Satz ist das Wort „Drehung" in einem weiteren Sinne genommen als gewöhnlich. Dies wird schon dadurch nahe gelegt, daß diese Drehung in einer affinen Transformation enthalten ist, und diese Transformationen unterscheiden sich sehr wesentlich, je nachdem die Transformationsdeterminante positiv oder negativ ist. In der Tat, ist $\bar{a}^2$ positiv, so ist in unserem Satz der Winkel

$$\hat{\alpha} = \tfrac{1}{2}\,\mathrm{Log}\,\frac{(a + b\sqrt{m})^2}{\bar{a}^2}$$

reell zu nehmen, und wir haben es nur mit einer gewöhnlichen Drehung zu tun. Ist aber $\bar{a}^2$ negativ, $\bar{a}$ also imaginär, so ist:

$$\hat{\alpha} = \tfrac{1}{2}i\pi + \tfrac{1}{2}\,\mathrm{Log}\left[-\frac{(a + b\sqrt{m})^2}{\bar{a}^2}\right]$$

ein komplexer Winkel, und zwischen Anfangs- und Endlage des Radius ist eine Asymptote gelegen. Man kann diese uneigentliche Drehung auffassen als die Kombination einer *eigentlichen Drehung* um den reellen Winkel $\tfrac{1}{2}\,\mathrm{Log}\left[-\frac{(a + b\sqrt{m})^2}{\bar{a}^2}\right]$, wobei der Radius aus einem Winkelraum der Asymptoten nicht heraustritt, und einer *Spiegelung* an einer Asymptote.

[Indem man einen Radius OP_1 sucht, der mit einem andern OP den Winkel $\tfrac{1}{2}i\pi$ einschließt, hat man geometrisch denjenigen Strahl im Büschel O zu bestimmen, der zusammen mit OP die Asymptoten harmonisch trennt.]

Zur Erläuterung diene beistehende Figur die dem Körper $k(\sqrt{10})$ mit der Klassenanzahl $h = 2$ entspricht.

Aus den Punkten $O = 0$, $\mathfrak{a} = 1$, $\mathfrak{b} = 1 + \sqrt{10}$, $\mathfrak{c} = \sqrt{10}$ gehen für das Punktgitter $(\alpha) = (1 + \sqrt{10})$ die Gitterpunkte hervor:

$$O = 0, \quad \mathfrak{A} = 1 + \sqrt{10}, \quad \mathfrak{B} = 11 + 2\sqrt{10}, \quad \mathfrak{C} = 10 + \sqrt{10}.$$

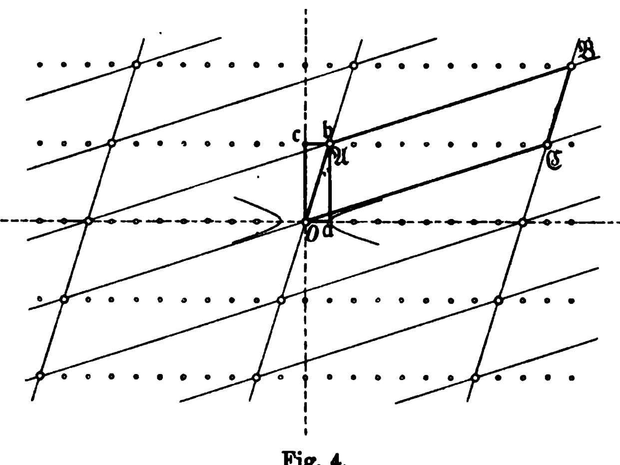


Fig. 4.

Durch Benützung unserer Formeln erhalten wir für den Winkel, den

$O\mathfrak{A}$ mit der x-Achse einschließt, $\varphi_{\mathfrak{A}} = \frac{1}{2}\,\mathrm{Log}\,\frac{1+\sqrt{10}}{1-\sqrt{10}}$

$O\mathfrak{B}$ „ „ „ „ $\varphi_{\mathfrak{B}} = \frac{1}{2}\,\mathrm{Log}\,\frac{11+2\sqrt{10}}{11-2\sqrt{10}}$

$O\mathfrak{C}$ „ „ „ „ $\varphi_{\mathfrak{C}} = \frac{1}{2}\,\mathrm{Log}\,\frac{10+\sqrt{10}}{10-\sqrt{10}}$

und finden schließlich $\sphericalangle\, \mathfrak{A}O\mathfrak{C} = \frac{1}{2}\,\mathrm{Log} - 1 = \sphericalangle\, \mathfrak{a}O\mathfrak{c}$. In analoger Weise berechnen sich die Winkel $O\mathfrak{A}\mathfrak{B} = O\mathfrak{a}\mathfrak{b}$, $\mathfrak{A}\mathfrak{B}\mathfrak{C} = \mathfrak{a}\mathfrak{b}\mathfrak{c}$ und $\mathfrak{B}\mathfrak{C}O = \mathfrak{b}\mathfrak{c}O$. Da zudem das Verhältnis besteht:

$$O\mathfrak{A} : O\mathfrak{C} = \sqrt{-9} : \sqrt{90} = \sqrt{-1} : \sqrt{10},$$
$$O\mathfrak{a} : O\mathfrak{c} = 1 : \sqrt{-10} = O\mathfrak{A} : O\mathfrak{C},$$

so sind im Sinne der getroffenen pseudometrischen Maßbestimmung die Figuren $O\mathfrak{a}\mathfrak{b}\mathfrak{c}$ und $O\mathfrak{A}\mathfrak{B}\mathfrak{C}$ als ähnlich zu bezeichnen.

Etwas erweitert lautet das eben erhaltene Resultat:

Das Gitter (α) ist dem Grundgitter ähnlich und geht aus diesem hervor durch eine Drehung um den Winkel $\widehat{\alpha} = \frac{1}{2}\,\mathrm{Log}\,\frac{a+b\sqrt{m}}{a-b\sqrt{m}}$ und eine Vergrößerung im Verhältnis $\bar{a} : 1$.

Genau wie im Falle des imaginären Körpers beweist man auch für das Punktgitter (α), daß man unendlich viele verschiedene Parallelgitter in dasselbe einlegen kann und daß irgend zwei dieser Parallelgitter durch eine affine Transformation mit der Determinante ± 1 ineinander übergeführt werden können.

Um indessen die Struktur eines Punktgitters (α) wirklich zu kennen, müssen wir hier eine besondere Behandlung der geometrischen Deutung der Einheitsideale des reellen Körpers einfügen.

Es ist früher bewiesen worden, daß in einem reellen Körper stets unendlich viele Grundeinheiten vorhanden sind. Die Bilder derselben liegen auf der Eichkurve und es entspricht speziell der Grundeinheit derjenige Einheitspunkt, welcher unter allen Einheitspunkten die kleinste Neigung besitzt.

Wir setzen zuerst voraus, daß ε eine Einheit des Körpers $k(\sqrt{m})$ ist, mit der Norm $n(\varepsilon) = +1$. Das Punktgitter (ε) besteht einfach wieder aus allen Gitterpunkten des Körpers. Nach der Darstellung des Ideals (α) andererseits geht das Punktgitter (ε) aus dem Punktgitter des Körpers durch eine Drehung um den Winkel

$$\widehat{\varepsilon} = \tfrac{1}{2} \operatorname{Log} \frac{a + b\sqrt{m}}{a - b\sqrt{m}} = \tfrac{1}{2} \operatorname{Log} (a + b\sqrt{m})^2$$

hervor, weil $\bar{e} = n(\varepsilon) = +1$ ist und daher eine Dehnung nicht vorgenommen wird. Ebenso erhält man aus dem Punktgitter des Körpers das Punktgitter (ε^k), wobei k eine ganze positive oder negative Zahl bezeichnet, durch eine Drehung um den Winkel $k \operatorname{Log}(a + b\sqrt{m})$ und das Punktgitter $(-\varepsilon^k)$ durch eine Drehung um $k \operatorname{Log}(a + b\sqrt{m}) + i\pi$. Weil aber die Punktgitter $(\pm \varepsilon^k)$ mit dem ursprünglichen Punktgitter immer wieder identisch sind, so läßt sich die Existenz der unendlich vielen Einheiten des Körpers durch folgende geometrische Deutung umschreiben:

Das Punktgitter der ganzen Zahlen des reellen Körpers $k(\sqrt{m})$ hat die Eigenschaft, durch eine Drehung um ein beliebiges (bis unendlich großes) ganzes Vielfaches des Winkels $\widehat{\varepsilon}$, also um $k\widehat{\varepsilon}$ oder auch um $i\pi + k\widehat{\varepsilon}$, in sich selbst überzugehen. Bei dieser Drehung bewegen sich die Einheitspunkte auf der Eichkurve und ein beliebiger Punkt auf einer zur (eigentlichen oder uneigentlichen) Eichkurve ähnlichen Hyperbel $x^2 - my^2 = C$.

Das Punktgitter eines reellen Körpers hat also ganz analoge Eigenschaften wie etwa ein reguläres Polygon, oder doch wie ein in einen Kreis eingeschriebenes Polygon mit gewissen Symmetrieeigenschaften.

Ferner sei ε eine Einheit des Körpers $k(\sqrt{m})$, deren Norm gleich -1 ist, dann bleibt natürlich die Behauptung richtig, daß das Punktgitter (ε) identisch ist mit dem Punktgitter des Körpers. Es geht aus diesem letzteren hervor durch eine, jetzt uneigentliche, Drehung um den Winkel:

$$\widehat{\varepsilon} = \tfrac{1}{2}\operatorname{Log}\frac{a+b\sqrt{m}}{a-b\sqrt{m}} = \operatorname{Log}(a+b\sqrt{m}) - \tfrac{1}{2}\operatorname{Log}(-1)$$
$$= -\tfrac{1}{2}i\pi + \operatorname{Log}(a+b\sqrt{m}),$$

d. h. durch eine Drehung verbunden mit einer Spiegelung an einer der Asymptoten, womit eine gleichzeitige Verwandlung der Radienvektoren im Verhältnis $\sqrt{-1}:1$ verbunden ist.

Das Punktgitter $(-\varepsilon)$ ist nur durch eine Spiegelung am Punkt 0 von dem Punktgitter (ε) verschieden.

Das Punktgitter (ε^2) geht aus dem ursprünglichen Gitter durch eine eigentliche Drehung hervor. Bei der Untersuchung der Einheitsgitter sind also die Einheiten ε^{2k+1} und ε^{2k} zu unterscheiden, übrigens aber läßt sich allgemein der folgende geometrische Satz formulieren:

Wenn der reelle Körper $k(\sqrt{m})$ eine Grundeinheit ε mit der Norm -1 enthält, und wenn $\varepsilon = ie^{\frac{i\pi}{2}+\widehat{\varepsilon}_1}$ gesetzt wird, wo nun $\widehat{\varepsilon}_1$ ein reeller Winkel ist, so geht das Punktgitter der ganzen Zahlen des Körpers durch eine Drehung um den Winkel $\widehat{\varepsilon}_1$ und eine darauf folgende Spiegelung an einer Asymptote der Eichkurve in sich über.

Die beiden eben angeführten geometrischen Deutungen erläutern die Bedeutung der Sätze über die Einheiten für den quadratischen Körper und machen das Interesse für den Unterschied der positiven oder negativen Norm der Grundeinheit verständlich.

Die Kenntnis der Einheiten des reellen Körpers ist analytisch betrachtet die Kenntnis aller linearen Transformationen mit ganzzahligen Koeffizienten

$$X = ax + bmy,$$
$$Y = bx + ay,$$

durch welche das Punktgitter des Körpers in sich übergeführt wird. Denn es ist klar, daß alle Transformationen dieser Art die Determinante ± 1 besitzen.

Für die imaginären Körper, mit Ausnahme etwa von $k(\sqrt{-3})$, ist die Aufsuchung dieser Transformationen eine triviale Aufgabe.

Der Körper $k(\sqrt{-1})$ liefert ein Grundgitter, welchem ein Parallelgitter mit *quadratischen* Maschen eingelagert werden kann. Dieses

Gitter geht durch Drehung um 90^0 und Spiegelung an den Winkelhalbierenden der Achsenwinkel in sich über. Das gleiche Resultat würde natürlich auch die geometrische Deutung der Eigenschaften der Einheiten $\pm\sqrt{-1}$ ergeben.

Es leuchtet nunmehr ohne weiteres ein, daß die Einheiten für ein Punktgitter (α) genau dieselbe Rolle spielen wie für das Zahlengitter selbst, denn es ist ja stets $(\alpha) = (\alpha\varepsilon)$. D. h. aber, die Einheiten liefern alle Drehungen (eigentliche und uneigentliche) oder, analytisch gesprochen, alle linearen Transformationen eines Punktgitters (α) in sich.

Damit haben wir nun aber alle Punkte zur Sprache gebracht, in denen die reellen Körper andere Resultate liefern als die imaginären Körper. Die bisherigen Auseinandersetzungen zeigen, welche Zusätze bei der Deutung der Ideale reeller Körper zu den entsprechenden Sätzen für imaginäre Körper noch zu machen sind. Wir dürfen insbesondere auch eine gesonderte Behandlung derjenigen Körper, in welchen $m \equiv 1, (4)$ ist, übergehen und können uns mit der Anführung des Schlußresultates begnügen:

Satz. *Ordnet man den ganzen Zahlen eines reellen Körpers die Punkte eines Punktgitters zu, so entspricht jedem Ideal* $\mathfrak{j}$ *des Körpers ein Punktgitter* $\mathfrak{j}$, *welchem unendlich viele Parallelgitter eingeschrieben werden können. Diese Parallelgitter werden durch affine Transformationen mit der Determinante* ± 1 *ineinander transformiert. Jedes Punktgitter läßt insbesondere unendlich viele Transformationen in sich zu, welche durch die Einheiten des Körpers geliefert werden.*

Die Masche eines Gitters enthält Gitterpunkte des Grundgitters, die einem vollständigen Restsystem mod $(\mathfrak{j})$ entsprechen.

Äquivalenten Idealen entsprechen ähnliche Gitter, so daß sich die sämtlichen Punktgitter auf h Klassen verteilen. Jede Klasse enthält mindestens ein Gitter mit einem Mascheninhalt $< \frac{d}{2}$.

Vierter Abschnitt.

Zahlkörper dritten Grades.

In den vorausgehenden Kapiteln habe ich die Theorie des quadratischen Zahlkörpers mit einiger Vollständigkeit behandelt. Es lag dabei die Absicht zugrunde, den Leser mit den Problemen aus der Theorie eines beliebigen Zahlkörpers bekannt zu machen. Aber der quadratische Zahlkörper ist doch so speziell, daß es meistens nicht empfehlenswert war, die *Methoden* der allgemeinen Körpertheorie zu seiner Untersuchung zu benutzen. Es hätte das geradezu den Vorwurf erwecken müssen, daß mit Kanonen nach Spatzen geschossen werde.

Dem Zweck des Buches entsprechend, das als Einführung in die Lehre von den algebraischen Zahlkörpern dienen soll, will ich nun wenigstens anhangsweise noch einige allgemeinere Methoden für die Begründung der Idealtheorie anführen. Hierzu behandle ich den Zahlkörper dritten Grades, soweit dies ohne neue größere Schwierigkeiten möglich ist, nämlich mit Ausschluß 1.) der Reziprozitätsgesetze und 2.) der Einteilung der Klassen in Geschlechter. Es sollen aber im folgenden nur diejenigen Beweise ausführlicher erörtert werden, welche sich *prinzipiell* von den Beweisen entsprechender Sätze für den quadratischen Zahlkörper unterscheiden. In einem weiteren Abschnitt will ich endlich noch den ungemein wichtigen und fruchtbaren Begriff des „Relativkörpers“ erklären, an dem Beispiel eines Relativkörpers in Beziehung auf einen quadratischen Grundkörper.

39. Grundbegriffe und Definitionen.

Die Begriffe des Zahlkörpers und der quadratischen Zahlen, die wir früher kennen gelernt haben, lassen sich ohne Schwierigkeit erweitern.

Jede Größe α, welche die Wurzel einer irreduziblen algebraischen Gleichung m^{ten} Grades mit rationalen Koeffizienten ist, heißt eine *algebraische Zahl.*

Adjungiert man diese algebraische Zahl α den rationalen Zahlen und führt nun in diesem durch α erweiterten Zahlsystem die Grundoperationen der Addition, Subtraktion, Multiplikation und Division beliebig oft aus, so erhält man einen neuen *Bereich* algebraischer Zahlen oder *Zahlkörper*. Derselbe besteht, anders ausgedrückt, aus den sämtlichen ganzen und gebrochenen rationalen Funktionen von α mit rationalen Koeffizienten. Der Zahlkörper hat folgende Fundamentaleigenschaften, die als Definition desselben gelten können:

1.) Die Summe oder Differenz irgend zweier Zahlen ist wieder eine Zahl des Zahlkörpers.

2.) Das Produkt oder der Quotient irgend zweier Zahlen ist wieder eine Zahl des Zahlkörpers.

Eine algebraische Zahl α ist eine *ganze* algebraische Zahl, wenn sie einer Gleichung m^{ten} Grades genügt:

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0,$$

in welcher $a_1, a_2, \ldots a_m$ *ganze* rationale Zahlen sind, während der Koeffizient von α^m gleich 1 ist.

Wir gehen nun gleich zum Zahlkörper dritten Grades (auch kubischer Zahlkörper genannt) über. Bei einigen Beweisen der folgenden Nummern benütze ich, z. T. ohne besondere Erklärung, verschiedene Sätze und Bezeichnungen aus der Algebra, wegen deren ich auf die Lehrbücher der Algebra verweise.

Es seien ϑ, ϑ', ϑ'' die Wurzeln der irreduziblen Gleichung dritten Grades:

$$G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0,$$

mit den ganzzahligen rationalen Koeffizienten a_1, a_2, a_3, so sind ϑ, ϑ', ϑ'' voneinander *verschiedene*, *ganze* algebraische Zahlen, die insbesondere nicht rational sind.

Die Zahlen ϑ, ϑ', ϑ'' sollen *konjugiert* heißen. Indem man der Reihe nach jede derselben dem Bereich der rationalen Zahlen adjungiert, erhält man drei verschiedene Zahlkörper mit den Zahlen θ, resp. θ' oder θ'', die ebenfalls *konjugiert* heißen. Diese Zahlkörper mögen mit $k(\vartheta)$, $k(\vartheta')$, $k(\vartheta'')$ bezeichnet werden; dann geht z. B. $k(\vartheta')$ aus dem Körper $k(\vartheta)$ hervor, wenn man in allen Zahlen des letzteren Körpers ϑ durch ϑ' ersetzt, oder die Substitution $S = S(\vartheta : \vartheta')$ ausführt.

Satz. *Die Zahlen des Körpers $k(\vartheta)$ können in der Form dargestellt werden:*

$$\theta = a + b\vartheta + c\vartheta^2,$$

wo a, b, c irgend welche rationalen Zahlen bedeuten.

In der Tat besteht der Körper $k(\vartheta)$ aus den sämtlichen rationalen, ganzen und gebrochenen Funktionen von ϑ, und es ist daher irgend eine Zahl θ des Körpers darstellbar in der Form:

$$\theta = \frac{f(\vartheta)}{f_1(\vartheta)},$$

wo f, f_1 nun als *ganze* rationale Funktionen beliebiger Grade, etwa r und r_1, mit *ganzzahligen* rationalen Koeffizienten vorausgesetzt werden können. Die Zahlen $f(\vartheta)$ und $f_1(\vartheta)$ sind hierbei von 0 verschieden angenommen. Alsdann sind die beiden Funktionen $f(x)$ und $f_1(x)$ prim zu $G(x)$, (d. i. sie haben mit $G(x)$ keinen Faktor $G_1(x) = b_0x^2 + b_1x + b_2$ gemeinsam). Denn, da $G(x)$ eine irreduzible Funktion ist, so könnte $f(x)$ resp. $f_1(x)$ nur durch $G(x)$ im ganzen teilbar sein, und es wäre daher $f(\vartheta) = 0$ resp. $f_1(\vartheta) = 0$ entgegen der Voraussetzung.

Nach einem Verfahren, welches dem Euklidischen Teilerverfahren nachgebildet ist, kann man jetzt zwei ganze rationale Funktionen $f_2(x)$ und $G_2(x)$ mit rationalen Koeffizienten, von den resp. Graden 2 und $r_1 - 1$ so bestimmen, daß

$$f_2(x)\cdot f_1(x) + G_2(x)\cdot G(x) = 1$$

ausfällt. Mit Rücksicht auf die Gleichung $G(\vartheta) = 0$ gilt danach die Gleichung:

$$\theta = \frac{f(\vartheta)}{f_1(\vartheta)} = \frac{f_2(\vartheta)f(\vartheta)}{f_2(\vartheta)f_1(\vartheta) + G_2(\vartheta)\,G(\vartheta)} = f_2(\vartheta)f(\vartheta) = F(\vartheta).$$

D. h. zunächst, daß jede Zahl des Zahlkörpers durch eine *ganze* rationale Funktion mit rationalen Koeffizienten darstellbar ist. Eine Funktion $F(x)$ von höherem als dem 2ten Grad kann aber stets auf die Form:

$$F(x) = F_1(x)\cdot G(x) + G_1(x)$$

gebracht werden, indem man $F(x)$ durch $G(x)$ dividiert, und wobei nun $G_1(x)$ eine Funktion höchstens vom zweiten Grade in x, mit rationalen Koeffizienten bezeichnet, die sich als Rest bei der Division von $F(x)$ durch $G(x)$ ergibt. Wegen $G(\vartheta) = 0$ ist aber $F(\vartheta) = G_1(\vartheta)$. Daher repräsentiert:

$$\theta = a + b\vartheta + c\vartheta^2$$

die *allgemeinste* Form der Zahlen aus $k(\vartheta)$, welche für spezielle Werte der Koeffizienten a, b, c die Zahlen des Zahlkörpers liefert.[1])

1) Aus der Darstellung von θ und der Tatsache, daß $\vartheta' + \vartheta''$, $\vartheta'\vartheta''$ stets auch dem Körper $k(\vartheta)$ angehören, folgt, daß auch $\theta' + \theta''$ und $\theta'\theta''$ dem Körper $k(\vartheta)$ angehören, ebenso wie θ selbst.

Hieraus folgt weiter:

Irgend eine nicht rationale Zahl θ des Körpers $k(\vartheta)$ genügt einer irreduziblen Gleichung dritten Grades mit rationalen Koeffizienten.

Es braucht jedoch diese Behauptung wohl nicht besonders bewiesen zu werden. Wir wenden uns gleich zur Untersuchung der *ganzen* Zahlen des Körpers. Für diese gilt der Satz:

Satz. *Die Summe, Differenz oder das Produkt von irgend zwei ganzen Zahlen des Körpers $k(\vartheta)$ ist wieder eine ganze Zahl desselben.*

Beweis. α und β seien zwei ganze Zahlen des Körpers, dann können wir jedenfalls schreiben:

$$\alpha = u + v\vartheta + w\vartheta^2,$$
$$\beta = u_1 + v_1\vartheta + w_1\vartheta^2,$$

wo u, v, w, u_1, v_1, w_1 rationale Zahlen sind. Es genügen ϑ, α, β bezw. den Gleichungen mit *ganzen* rationalen Koeffizienten:

$$G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0 \tag{1}$$
$$x^3 + A_1x^2 + A_2x + A_3 = 0 \tag{2}$$
$$x^3 + B_1x^2 + B_2x + B_3 = 0. \tag{3}$$

Für die Summe $\alpha + \beta$ z. B. ist von vornherein klar, daß sie einer Gleichung vom dritten Grad mit rationalen Koeffizienten genügt. Denn die Koeffizienten der Gleichung:

$$S(x) = [x - (\alpha + \beta)][x - (\alpha' + \beta')][x - (\alpha'' + \beta'')] = 0 \tag{4}$$

lassen sich rational und *ganz* durch u, v, w, u_1, v_1, w_1 und die elementaren symmetrischen Funktionen der $\vartheta, \vartheta', \vartheta''$ nämlich a_1, a_2, a_3, ausdrücken. Der Koeffizient von x^3 in $S(x)$ ist gleich 1, man hat daher nur noch zu beweisen, daß die übrigen Koeffizienten *ganze* rationale Zahlen sind.

Zu diesem Zweck bilde man zunächst die Gleichung neunten Grades:

$$T(x) = [x - (\alpha + \beta)][x - (\alpha + \beta')][x - (\alpha + \beta'')] \dots$$
$$[x - (\alpha'' + \beta)][x - (\alpha'' + \beta')][x - (\alpha'' + \beta'')] = 0. \tag{5}$$

In dem Ausdruck $T(x)$ ist alsdann der Koeffizient des höchsten Gliedes 1, alle übrigen Koeffizienten sind ganze rationale symmetrische Funktionen der $\alpha, \alpha', \alpha''$ und β, β', β'' und drücken sich daher rational und *ganz* durch die Koeffizienten der Gleichungen (2) und (3), d. h. durch die ganzen rationalen Zahlen A resp. B, aus. Es sind also die Koeffizienten in $T(x)$ auch ganze rationale Zahlen, und es wäre schon damit gezeigt, daß $\alpha + \beta$ eine ganze Zahl ist. Jedoch kann weiter so geschlossen werden:

Die Funktion $S(x)$ auf der linken Seite der Gleichung (4) ist ein Faktor von $T(x)$, oder $T(x)$ muß in das Produkt zweier ganzer rationaler Funktionen $S(x)$ und $S_1(x)$ zerfallen:

$$T(x) = S(x) \cdot S_1(x).$$

Weil nun die Koeffizienten von $T(x)$ und $S(x)$ rationale Zahlen sind, so müssen auch die Koeffizienten von $S_1(x)$ rational sein, und zwar ist der Koeffizient des höchsten Gliedes in $S_1(x)$ gleich 1. Es ergibt sich dies aus der letzten Gleichung, wenn man

$$S_1(x) = \frac{T(x)}{S(x)}$$

setzt.

Nun folgt aus einem Satz von Gauß[1]), daß auch alle Koeffizienten in $S(x)$ und $S_1(x)$ *ganze* rationale Zahlen sein müssen, da ja die Koeffizienten in $T(x)$ ganz sind.

Damit ist aber der Satz für die Summe (und Differenz) irgend zweier ganzer Zahlen bewiesen.

Für das Produkt zweier ganzer Zahlen treten an Stelle der Gleichungen (4) und (5) die Gleichungen:

$$P(x) = (x - \alpha\beta)(x - \alpha'\beta')(x - \alpha''\beta'') = 0, \qquad (4\text{a})$$

$$Q(x) = (x - \alpha\beta)(x - \alpha\beta')(x - \alpha\beta'')$$

$$(x - \alpha'\beta)(x - \alpha'\beta')(x - \alpha'\beta'')(x - \alpha''\beta)(x - \alpha''\beta')(x - \alpha''\beta'') = 0. \qquad (5\text{a})$$

Im übrigen aber bleiben alle Schlüsse wörtlich dieselben wie oben.

Durch wiederholte Anwendung des vorstehenden Satzes auf 3, 4, ... m Zahlen folgt die Richtigkeit der allgemeinen Behauptung:

Satz. *Jede ganze rationale Funktion von beliebig vielen ganzen Zahlen des Körpers mit ganzzahligen rationalen Koeffizienten ist wieder eine ganze Zahl des Körpers.*

---

1) Vergl. z. B. H. Weber, Lehrbuch der Algebra, 2. Aufl. Braunschweig 1898. Bd. I, S. 98:

Sind
$$\varphi(x) = x^m + a_1 x^{m-1} + \cdots + a_m$$
$$\psi(x) = x^n + b_1 x^{n-1} + \cdots + b_n$$

zwei ganze rationale Funktionen, in denen die höchsten Potenzen von x den Koeffizienten 1 haben, während die übrigen Koeffizienten rationale Zahlen sind, so können in dem Produkt

$$\varphi(x) \cdot \psi(x) = x^{m+n} + c_1 x^{m+n-1} + \cdots + c_{m+n}$$

die Koeffizienten $c_1, c_2, c_3, \ldots c_{m+n}$ nicht alle ganze Zahlen sein, wenn die Koeffizienten a, b in $\varphi(x)$ und $\psi(x)$ nicht alle ganze Zahlen sind.

Eine wichtige Folgerung aus diesen Überlegungen ist die, daß außer einer ganzen Zahl α auch stets $\alpha'\alpha''$ eine ganze Zahl des Körpers sein muß. Denn es ist $\alpha'\alpha'' = \frac{n(\alpha)}{\alpha}$ eine ganze Zahl, und $\frac{n(\alpha)}{\alpha}$ gehört dem Körper $k(\vartheta)$ an.

In einem der folgenden Sätze wird die Tatsache benutzt:

Satz. *Wenn eine ganze Zahl des Zahlkörpers $k(\vartheta)$ eine rationale Zahl ist, so ist sie zugleich eine ganze rationale Zahl.*

Beweis. Der Beweis dieser Behauptung ergibt sich aus dem soeben zitierten Satz von Gauß, wenn man berücksichtigt, daß die Gleichung 3ten Grades für die ganze rationale Zahl α zerfällbar sein muß.

40. Die Diskriminante einer ganzen Zahl des Körpers.

Wenn α eine beliebige ganze Zahl des Zahlkörpers $k(\vartheta)$ ist, so gelten folgende Bezeichnungen:

1.) Die Zahlen α', α'', welche aus α dadurch hervorgehen, daß man ϑ durch ϑ', dann ϑ durch ϑ'' ersetzt, heißen *konjugiert* zu α.

2.) Das Produkt der drei konjugierten Zahlen α, α', α'', oder:

$$n(\alpha) = \alpha\alpha'\alpha''$$

heißt die *Norm* der Zahl α.

3.) Das Produkt:

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'')$$

heißt die *Differente* der Zahl α.

4.) Das Produkt

$$d(\alpha) = (\alpha - \alpha')^2(\alpha - \alpha'')^2(\alpha' - \alpha'')^2$$
$$= \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha' & \alpha'^2 \\ 1 & \alpha'' & \alpha''^2 \end{vmatrix}^2$$

heißt die *Diskriminante* der Zahl α.

Die Norm und die Diskriminante einer *ganzen* Zahl α sind *ganze rationale Zahlen*, sie gehören dem Zahlkörper an. Auch die Differente der Zahl α ist eine Zahl des Körpers, denn es ist:

$$\delta(\alpha) = \alpha^2 - \alpha(\alpha' + \alpha'') + \alpha'\alpha''.$$

Ferner besteht zwischen der Diskriminante und der Differente einer Zahl die Beziehung:

$$d(\alpha) = -n(\delta(\alpha)).$$

Die Diskriminante der Zahl ϑ, welche den Körper $k(\vartheta)$ bestimmt, ist bekanntlich eine ganze rationale Funktion von a_1, a_2, a_3. Diese Funktion verschwindet nicht, da $G(x)$ als irreduzible Funktion vorausgesetzt wurde, d. h. da $G(x) = 0$ keine Doppelwurzel besitzen darf.

Aus der Algebra ist bekannt, wie man die Größe $d(\alpha)$ durch die elementaren symmetrischen Funktionen berechnet. Für ϑ, welches eine Wurzel der Gleichung $G(x) = 0$ ist, ergibt sich:

$$d(\vartheta) = a_1^2 a_2^2 + 18 a_1 a_2 a_3 - 4 a_2^3 - 4 a_1^3 a_3 - 27 a_3^2.$$

Wenn insbesondere $a_1 = 0$ ist, so bleibt für $d(\vartheta)$ der einfache Ausdruck übrig:

$$d(\vartheta) = -4 a_2^3 - 27 a_3^2.$$

Die Diskriminante einer rationalen Zahl ist offenbar stets gleich Null. Falls umgekehrt die Diskriminante $d(\alpha)$ einer ganzen Zahl α verschwindet, so ist diese Zahl rational. In der Tat, wenn $d(\alpha) = 0$ wird, so ist $\alpha = \alpha' = a$ usw., oder man kann zwei rationale Zahlen b, c so angeben, daß $\alpha^2 + b\alpha + c = 0$ wird. Dies ist aber nur möglich, wenn α rational ist. Jede nicht rationale Zahl α des Körpers genügt einer irreduziblen Gleichung dritten Grades.

Im Falle die Diskriminante der Zahl ϑ, welche den Körper bestimmt, positiv ist, sind alle Wurzeln der Gleichung $G(x) = 0$ *reell;* die drei konjugierten Körper $k(\vartheta)$, $k(\vartheta')$, $k(\vartheta'')$ enthalten alsdann nur reelle Zahlen und sollen *reelle* Körper heißen.

Falls aber die Diskriminante $d(\vartheta)$ negativ ist, besitzt die Gleichung $G(x) = 0$ nur eine reelle und zwei konjugiert imaginäre (komplexe) Wurzeln. Einer der drei konjugierten Körper enthält dann lauter reelle Zahlen und ist ein reeller Körper, die beiden anderen Körper enthalten komplexe Zahlen und sollen *imaginäre* Körper heißen.

Satz. *Die Diskriminante jeder nicht rationalen ganzen Zahl eines Zahlkörpers vom dritten Grad ist stets verschieden von Null und von* ± 1.

Beweis. Die Diskriminanten aller von Null verschiedenen, nicht rationalen ganzen Zahlen eines Körpers besitzen dasselbe Vorzeichen. Denn ist:

$$\alpha = a_1 + b_1 \vartheta + c_1 \vartheta^2,$$
$$\alpha^2 = a_2 + b_2 \vartheta + c_2 \vartheta^2,$$

so ist nach dem Produktsatze für Determinanten:

$$d(\alpha) = (b_1 c_2 - b_2 c_1)^2 \cdot d(\vartheta).$$

Da der erste Faktor der rechten Seite stets positiv und von Null ver-

schieden ist, so hat die Diskriminante $d(\alpha)$ einer jeden Zahl α das gleiche Vorzeichen wie $d(\vartheta)$.

Als ganze, nicht rationale Zahl des Körpers genügt α einer irreduziblen Gleichung dritten Grades:

$$x^3 + u_1 x^2 + u_2 x + u_3 = 0, \tag{1}$$

mit ganzen rationalen Koeffizienten. Entweder ist hierin $u_1 = 0$, und es wird $d(\alpha) = -4u_2^3 - 27u_3^2$, oder es ist u_1 verschieden von Null, dann kann man die Gleichung (1) durch die Substitution:

$$y = x + \frac{u_1}{3} \quad \text{oder} \quad x = y - \frac{u_1}{3},$$

auf die Form:

$$y^3 + \frac{U_2}{3} y + \frac{U_3}{27} = 0, \tag{2}$$

bringen, in welcher U_2, U_3 ganze rationale Zahlen sind. Hierbei ist U_2 durch 3 und U_3 durch 27 teilbar, wenn u_1 durch 3 teilbar ist. Wenn dies der Fall ist, so hat $d(\alpha)$ einfach wieder die Form $-4u_2^{*3} - 27u_3^{*2}$. Falls $u_1 \not\equiv 0, (3)$ ist, so wird:

$$d(\alpha) = -4\frac{U_2^3}{27} - 27\frac{U_3^2}{27^2} = -\frac{1}{27}(4U_2^3 + U_3^2).$$

Wenn nun die Diskriminante einer ganzen Zahl gleich -1 vorausgesetzt wird, so müßte daher eine der beiden Gleichungen:

$$4u_2^3 + 27u_3^2 = 1 \tag{3}$$

$$4U_2^3 + U_3^2 \;\; = 27 \tag{4}$$

für ganze Zahlen u, U bestehen, und folglich würde eine der beiden Kongruenzen:

$$27u_3^2 - 1 \equiv 0,\ (4) \quad \text{oder} \quad U_3^2 - 27 \equiv 0,\ (4)$$

lösbar sein. Da dies aber augenscheinlich nicht zutrifft, so ist auch die Voraussetzung $d(\alpha) = -1$ nicht zulässig.

Es kann aber auch nicht $d(\alpha) = +1$ werden. In der Tat hat sich aus der Unlösbarkeit der Diophantischen Gleichung: $x^3 + y^3 = z^3$ ergeben, daß die Gleichungen:

$$y^3 - y \pm \tfrac{1}{3} = 0, \tag{5}$$

die einzigen Gleichungen sind mit rationalen Koeffizienten und der Wurzelsumme Null, für welche die Diskriminante $d(\alpha)$ gleich $+1$ wird. Diese Gleichungen definieren aber keine ganzen algebraischen Zahlen. Es gibt auch keine Substitution $y = x + \frac{u_1}{3}$, durch welche man aus der Gleichung (5) eine andere Gleichung:

$$x^3 + u_1 x^2 + u_2 x + u_3 = 0$$

mit lauter *ganzen* rationalen Koeffizienten ableiten könnte, wie man durch Einsetzen des Wertes für y in die Gleichung (5) sofort erkennt.

41. Die Basis des Körpers $k(\vartheta)$.

Für die Darstellung der ganzen Zahlen des Körpers ist nun der folgende Satz von größter Bedeutung:

Satz. *In dem Zahlkörper $k(\vartheta)$ kann man stets, und zwar auf unendlich viele Weisen, drei ganze Zahlen ω_1, ω_2, ω_3 so auswählen, daß jede beliebige ganze Zahl des Körpers in der Form darstellbar ist:*

$$x\omega_1 + y\omega_2 + z\omega_3,$$

worin x, y, z ganze rationale Zahlen bedeuten.

Beweis. Der Beweis zerfällt in zwei Teile. Man stellt zunächst die *allgemeine* Form auf, in welcher sich die ganzen Zahlen des Körpers darstellen lassen, und leitet dann daraus drei Zahlen der verlangten Art ab.

Bezeichnen a, b, c ganze rationale Zahlen, so folgt unmittelbar aus dem Satz auf S. 247, daß die algebraischen Zahlen $a + b\vartheta + c\vartheta^2$ ganz sind, da nach Voraussetzung ϑ eine ganze Zahl des Körpers bezeichnet.

Es seien nun a, b, c ganz allgemein, irgend welche rationalen Zahlen und

$$\alpha = a + b\vartheta + c\vartheta^2,$$

so ist die Frage, welche Bedingung haben die rationalen Koeffizienten a, b, c zu erfüllen, damit α eine ganze Zahl des Körpers ist? Wenn α ganz ist, so sind auch die konjugierten Zahlen α', α'' ganz. Berechnet man nun umgekehrt a, b, c aus den 3 Gleichungen:

$$\left.\begin{aligned} a + b\vartheta + c\vartheta^2 &= \alpha \\ a + b\vartheta' + c\vartheta'^2 &= \alpha' \\ a + b\vartheta'' + c\vartheta''^2 &= \alpha'' \end{aligned}\right\}, \tag{1}$$

dann erhält man:

$$a = \frac{\begin{vmatrix} \alpha & \vartheta & \vartheta^2 \\ \alpha' & \vartheta' & \vartheta'^2 \\ \alpha'' & \vartheta'' & \vartheta''^2 \end{vmatrix}}{\begin{vmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \vartheta' & \vartheta'^2 \\ 1 & \vartheta'' & \vartheta''^2 \end{vmatrix}} = \frac{\begin{vmatrix} \alpha & \vartheta & \vartheta^2 \\ \alpha' & \vartheta' & \vartheta'^2 \\ \alpha'' & \vartheta'' & \vartheta''^2 \end{vmatrix} \begin{vmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \vartheta' & \vartheta'^2 \\ 1 & \vartheta'' & \vartheta''^2 \end{vmatrix}}{\begin{vmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \vartheta' & \vartheta'^2 \\ 1 & \vartheta'' & \vartheta''^2 \end{vmatrix}^2}, \tag{2}$$

sowie ähnliche Ausdrücke für b, c.

Die rationalen Größen a, b, c lassen sich also darstellen als Brüche, deren Zähler und Nenner ganze rationale Funktionen der ganzen Zahlen α, α', α'', ϑ, ϑ', ϑ'' sind. Die Nenner aller drei Größen a, b, c sind hierbei gleich $d(\vartheta)$, somit ganze rationale Zahlen, ebenso sind auch die drei Zähler selbst rationale und daher nach dem Satz auf S. 248 zugleich ganze rationale Zahlen.

Anders ausgedrückt erhält man also das Resultat: wenn $\alpha = a + b\vartheta + c\vartheta^2$ eine ganze Zahl darstellt, so können die Nenner der Koeffizienten a, b, c nur solche Primfaktoren enthalten, welche auch in $d(\vartheta)$ aufgehen. Man darf a, b, c stets in der Form annehmen:

$$a = \frac{A}{d(\vartheta)}, \qquad b = \frac{B}{d(\vartheta)}, \qquad c = \frac{C}{d(\vartheta)},$$

wo jetzt A, B, C ganze rationale Zahlen sind.

Aus der hiermit gewonnenen Darstellung der ganzen Zahlen:

$$\alpha = \frac{A + B\vartheta + C\vartheta^2}{d(\vartheta)} \tag{3}$$

ergibt sich nun die Bestimmung der Zahlen ω_1, ω_2, ω_3. Wenn man sich alle ganzen Zahlen des Körpers in der Form

$$\frac{a + b\vartheta + c\vartheta^2}{d(\vartheta)}$$

angeschrieben denkt (wo von jetzt ab a, b, c wieder nur ganze rationale Zahlen bedeuten sollen), so gibt es jedenfalls unendlich viele solcher Zahlen, in welchen der Koeffizient von ϑ^2 nicht Null ist. Jede Zahl $\frac{a + b\vartheta + c\vartheta^2}{d(\vartheta)}$ kann man zunächst in zwei Teile zerlegen. Dividiert man $d(\vartheta)$ in a, b, c und nimmt dabei den Rest A, bezw. B, bezw. C absolut genommen $\leqq |d(\vartheta)|$, setzt also $a = a_1 d(\vartheta) + A$ usw., so wird:

$$\frac{a + b\vartheta + c\vartheta^2}{d(\vartheta)} = a_1 + b_1\vartheta + c_1\vartheta^2 + \frac{A + B\vartheta + C\vartheta^2}{d(\vartheta)} = \alpha_1 + \alpha,$$

α_1 und α sind ganze Zahlen des Körpers. Wir wollen im nächstfolgenden unter den Zahlen $\alpha = \frac{A + B\vartheta + C\vartheta^2}{d(\vartheta)}$ nur noch alle diejenigen *ganzen Zahlen* verstehen, für welche die Koeffizienten A, B, C ihren absoluten Beträgen nach $\leqq |d(\vartheta)|$ sind (Gleichheit ausdrücklich inbegriffen). Ist C^* der größte ganze gemeinsame Teiler aller der Koeffizienten C, mithin C^* eine ganz bestimmte Zahl $\geqq 1$, so existieren im Körper auch ganze Zahlen von der Form:

$$\alpha^* = \frac{A^* + B^*\vartheta + C^*\vartheta^2}{d(\vartheta)}. \tag{4}$$

Sind nämlich α_1, α_2 ganze Zahlen von der oben gefundenen Form:

$$\alpha_1 = \frac{a_1 + b_1\vartheta + c_1\vartheta^2}{d(\vartheta)} \quad \text{und} \quad \alpha_2 = \frac{a_2 + b_2\vartheta + c_2\vartheta^2}{d(\vartheta)}$$

und ist t der größte gemeinsame Teiler der beiden ganzen rationalen Zahlen c_1 und c_2, so kann man zwei ganze rationale Zahlen u, v derart bestimmen, daß $uc_1 + vc_2 = t$ ist und folglich

$$u\alpha_1 + v\alpha_2 = \frac{(ua_1 + va_2) + (ub_1 + vb_2)\vartheta + t\vartheta^2}{d(\vartheta)}$$

wird. Die Zahl $u\alpha_1 + v\alpha_2$ ist aber ebenfalls eine ganze Zahl des Körpers, wenn α_1, α_2 ganze Zahlen sind. Kombiniert man in derselben Weise, wie es eben mit α_1, α_2 geschah, die Zahlen

$$\alpha = \frac{A + B\vartheta + C\vartheta^2}{d(\vartheta)},$$

welche in endlicher Anzahl vorhanden sind, so kann man die Multiplikatoren $u, v, w, \ldots$ stets auf verschiedene Weisen derart wählen, daß man eine ganze Zahl von der Form der Zahl α^* erhält, mit C^* als einem bestimmten Koeffizienten von ϑ^2.

Die Zahl C^* ist selbst ein Faktor von $d(\vartheta)$, denn nach Voraus-aussetzung befindet sich unter den Zahlen α auch die ganze Zahl ϑ^2, für welche $C = d(\vartheta)$ zu setzen ist. Bezeichnet ferner $\frac{a + b\vartheta + c\vartheta^2}{d(\vartheta)}$ irgend eine ganze Zahl des Körpers, so muß auch c ein Vielfaches von C^* sein, weil $c = c_1 d(\vartheta) + C$ ist.

Wir denken uns nun unter α^* eine bestimmte ganze Zahl, indem wir außer C^* auch A^*, B^* als feste Zahlen voraussetzen, und schreiben ω_3 anstatt α^*. Dann kann *jede beliebige ganze Zahl*

$$\alpha = \frac{a + b\vartheta + c\vartheta^2}{d(\vartheta)}$$

auf die Form

$$\alpha = \frac{a_1 + b_1\vartheta}{d(\vartheta)} + z\omega_3$$

gebracht werden, wo z eine ganze rationale Zahl und $\frac{a_1 + b_1\vartheta}{d(\vartheta)}$ eine ganze Zahl des Körpers ist.

Wir verstehen nun unter:

$$\beta = \frac{A_1 + B_1\vartheta}{d(\vartheta)} \tag{5}$$

wiederum nur diejenigen ganzen Zahlen, deren Koeffizienten ihrem absoluten Betrag nach $\leq |d(\vartheta)|$ sind. Operiert man dann mit diesen Zahlen β genau ebenso, wie es vorhin mit den Zahlen α geschehen

ist, und bedeutet B_1^* den größten gemeinsamen Teiler der endlich vielen ganzen rationalen Zahlen B_1, so folgt, daß der Körper $k(\vartheta)$ stets ganze Zahlen von der Form

$$\beta^* = \frac{A_1^* + B_1^* \vartheta}{d(\vartheta)} \tag{6}$$

enthält.

Seiner Ableitung nach muß auch B_1^* ein Faktor von $d(\vartheta)$ sein, und falls $\frac{a_1 + b_1 \vartheta}{d(\vartheta)}$ irgend eine ganze Zahl bedeutet, so ist b_1 ein Vielfaches von B_1^*.

Es möge jetzt auch der Koeffizient A_1^* in der Gleichung (6) eine feste Zahl sein, und für β^* sodann ω_2 geschrieben werden. Dann läßt sich endlich jede Zahl $\beta = \frac{a_1 + b_1 \vartheta}{d(\vartheta)}$ in der Form $\beta = A_2 + y\omega_2$ darstellen, wo jetzt A_2 *und* y ganze rationale Zahlen sind.

Setzt man schließlich noch $\omega_1 = 1$, dann entsprechen die drei Zahlen ω_1, ω_2, ω_3 den Bedingungen des Satzes. Jede beliebige ganze Zahl α des Körpers läßt sich darstellen in der Form:

$$\alpha = x\omega_1 + y\omega_2 + z\omega_3. \tag{7}$$

Denn man kann zunächst z als ganze rationale Zahl so wählen, daß $\alpha - z\omega_3$ die Form der Zahl β in Gleichung (5) erhält. Sodann ist ferner y als ganze rationale Zahl derart bestimmbar, daß

$$\beta - y\omega_2 = \gamma$$

eine rationale Zahl wird, daher kann $\gamma = x\omega_1 = x$ gesetzt werden.

Durch Zusammenziehung der drei letzten Gleichungen folgt die Richtigkeit der Behauptung.

Man sagt, daß irgend drei ganze Zahlen des Körpers, welche dieselbe Eigenschaft besitzen wie ω_1, ω_2, ω_3, eine **Basis des Körpers** bilden.

An Stelle der drei Zahlen ω_1, ω_2, ω_3 kann man natürlich auch:

$$\omega = 1, \qquad \omega_1 = \frac{B + B_1 \vartheta}{d(\vartheta)}, \qquad \omega_2 = \frac{C + C_1 \vartheta + C_2 \vartheta^2}{d(\vartheta)}$$

als eine *Normalbasis* so wählen, daß $|B|$, bezw. $|C|$, $|C_1| < |d(\vartheta)|$ sind, oder überhaupt den absolut kleinsten Werten von A_1^* in Gl. (6) usw. entsprechen, und wo der bequemeren Schreibweise wegen $B_1 = B_1^*$ und $C_2 = C^*$ gesetzt ist.

Bilden ω_1, ω_2, ω_3 eine Basis des Körpers und ω_1^*, ω_2^*, ω_3^* eine davon verschiedene neue Basis, so bestehen zwischen diesen Zahlentripeln Gleichungen mit ganzzahligen Koeffizienten von folgender Form:

$$\left.\begin{aligned} \omega_1^* &= a_{11}\omega_1 + a_{12}\omega_2 + a_{13}\omega_3 \\ \omega_2^* &= a_{21}\omega_1 + a_{22}\omega_2 + a_{23}\omega_3 \\ \omega_3^* &= a_{31}\omega_1 + a_{32}\omega_2 + a_{33}\omega_3 \end{aligned}\right\}. \tag{8}$$

Da ferner auch umgekehrt die ω durch ω^* in derselben Weise ausdrückbar sein müssen, so gilt für die Koeffizienten a_{ik} die Beziehung:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \pm 1.$$

Wählt man andererseits die a_{ik} als ganze rationale Zahlen dieser letzten Bedingung gemäß, dann erhält man durch die 3 Gleichungen (8) eine neue Basis. Weil die a_{ik} auf unendlich viele verschiedene Weisen der letzten Gleichung gemäß gewählt werden können, existieren unendlich viele verschiedene andere Zahlentripel, die eine Basis des Körpers bilden.

Der Wert der Determinante:

$$d = \begin{vmatrix} \omega_1 & \omega_2 & \omega_3 \\ \omega_1' & \omega_2' & \omega_3' \\ \omega_1'' & \omega_2'' & \omega_3'' \end{vmatrix}^2 \tag{9}$$

heißt die *Diskriminante* des Körpers.

Aus dem Multiplikationssatz für Determinanten folgt, daß die Diskriminante des Körpers $k(\vartheta)$ unabhängig ist von der speziell gewählten Basis. Nach der üblichen abkürzenden Schreibweise für eine Determinante, durch Nebeneinanderstellung der von links oben nach rechts unten gehenden Diagonalglieder, ist nämlich unter Voraussetzung der Gleichungen (8) zwischen den Zahlen ω^* und ω:

$$(\omega_1^*, \omega_2^{*\prime}, \omega_3^{*\prime\prime})^2 = (a_{11}, a_{22}, a_{33})^2(\omega_1, \omega_2', \omega_3'')^2 = d.$$

Die Diskriminante des Körpers ist eine ganze rationale Zahl. Sie ist ein gemeinsamer Teiler aller Diskriminanten der ganzen Zahlen des Körpers. Denn für eine beliebige ganze Zahl α gilt stets eine Gleichung:

$$d(\alpha) = (x, y_1, z_2)^2 . d,$$

falls 1, α, α^2 folgendermaßen durch die Basis ausgedrückt sind:

$$\left.\begin{aligned} 1 &= x\,\omega_1 + y\,\omega_2 + z\,\omega_3 \\ \alpha &= x_1\omega_1 + y_1\omega_2 + z_1\omega_3 \\ \alpha^2 &= x_2\omega_1 + y_2\omega_2 + z_2\omega_3 \end{aligned}\right\}. \tag{10}$$

Bezeichnen $\omega, \omega_1, \omega_2$, eine Normalbasis des Körpers, ist also:

$$\omega = 1, \qquad \omega_1 = \frac{B + B_1 \vartheta}{d(\vartheta)}, \qquad \omega_2 = \frac{C + C_1 \vartheta + C_2 \vartheta^2}{d(\vartheta)},$$

so ergibt sich:

$$d = \frac{B_1{}^2 C_2{}^2}{d(\vartheta)^3}. \tag{11}$$

Nachdem früher schon gezeigt worden ist, daß B_1 und C_2 in $d(\vartheta)$ aufgehen müssen, folgt aus der Gleichung (11) nochmals, daß d nur Faktoren besitzen kann, welche auch in $d(\vartheta)$ aufgehen.

Ferner ergibt sich aus der Gleichung $d = \frac{B_1{}^2 C_2{}^2}{d(\vartheta)^3}$, daß die Diskriminante des Körpers alle diejenigen rationalen Primzahlen sicher als Faktoren enthält, welche in der Diskriminante der Zahl ϑ zu *ungerader* Potenz vorkommen.

Stimmt die Diskriminante d des Körpers überein mit der Diskriminante der den Körper definierenden Zahl ϑ, und setzt man in dem Gleichungssystem (10) die Zahl ϑ anstatt α, so wird $(x, y_1, z_2) = \pm 1$; d. h. die drei Zahlen 1, ϑ, ϑ^2 stellen selbst eine Basis des Körpers dar.

Eine genauere Diskussion der Behauptung, daß d und $\frac{d(\vartheta)}{d}$ ganze rationale Zahlen sind, ergibt, daß jedenfalls dann $d = d(\vartheta)$ wird, wenn die Diskriminante $d(\vartheta)$ alle Primfaktoren nur zur *ersten* Potenz enthält.

Aus dem Satze über die Diskriminanten der ganzen Zahlen des Körpers, nach dem $d(\vartheta)$ nicht gleich ± 1 werden kann, und mit Rücksicht auf die oben aufgestellte Basis eines Körpers $k(\vartheta)$, folgt jetzt unmittelbar, daß die Diskriminante d des Körpers sicher dann verschieden von ± 1 ausfällt, wenn $d(\vartheta)$ keine Quadratzahl ist. Wenn aber die Diskriminante $d(\vartheta)$ eine positive oder negative Quadratzahl ist, etwa $d(\vartheta) = \pm r^2$, so wäre nach dem Bisherigen nicht ausgeschlossen, daß $d = \pm 1$ wird.

Man könnte wohl noch durch eine direkte Methode, welche die verschiedenen möglichen Spezialfälle sonderte, den Nachweis führen, daß dies nicht eintritt. Es hat aber kein Interesse und ist unnötig, diesen direkten Beweis hier zu geben, da durch den Satz von Minkowski über lineare Formen ganz allgemein der Nachweis für die Behauptung möglich ist, daß die Diskriminante *jedes* Zahlkörpers verschieden von ± 1 ist.

Es wird dabei zuerst gezeigt, daß in jedem Körper eine ganze Zahl α existiert, für welche $|n(\alpha)| < |\sqrt{d}|$ ist. Da aber stets $|n(\alpha)| \geq 1$ ausfällt, so folgt notwendig $|d| > 1$.

Der Leser möge den verhältnismäßig kurzen Beweis dieses Satzes nachlesen bei Hilbert, Ber., Kap. VI, § 18, S. 211.

42. Die Berechnung der Basis des Zahlkörpers $k(\vartheta)$.

Die Aufstellung einer Basis für den Zahlkörper dritten Grades ist nicht mehr so einfach wie für den quadratischen Zahlkörper. Man kann aber doch auf Grund der Sätze über die Diskriminanten der ganzen Zahlen der Körperbasis eine Gestalt geben, aus welcher im speziellen numerischen Fall die wirkliche Basis unschwer selbst in Zahlen zu berechnen ist.[1])

Es sei zunächst wieder die Basis des Körpers:

$$\omega = 1, \qquad \omega_1 = \frac{B + B_1\vartheta}{d(\vartheta)}, \qquad \omega_2 = \frac{C + C_1\vartheta + C_2\vartheta^2}{d(\vartheta)}.$$

Weiter möge gesetzt werden:

$d(\vartheta) = \pm\, q_1^{6e_1} \ldots q^{6e} p_1^{f_1} \ldots p^f$, $\quad$ ($d(\vartheta)$ ist stets verschieden von ± 1),

wo die $e_1 \ldots e$ beliebige ganze Zahlen $\geqq 0$, $f_1 \ldots f$ aber nur die Zahlen 1, oder 2, ... 5 bedeuten sollen, so daß also die in $d(\vartheta)$ etwa enthaltene sechste Potenz einer ganzen Zahl abgesondert ist. Nun ist die Diskriminante der Basiszahl ω_1:

$$d(\omega_1) = \frac{B_1^6}{d(\vartheta)^5};$$

weil $d(\omega_1)$ eine *ganze*, von ± 1 verschiedene Zahl ist, B_1 aber nur Primfaktoren aus $d(\vartheta)$ enthält, so kann daher für B_1 offenbar folgender Ausdruck gesetzt werden:

$$B_1 = b^* q_1^{5e_1} \ldots q^{5e} \,.\, p_1^{f_1} \ldots p^f = b^* \,.\, b_1^*.$$

Hierin ist b^* entweder gleich ± 1, oder es bedeutet eine durch irgendwelche der Primfaktoren q, p teilbare ganze Zahl.

Damit wird aber:

$$\omega_1 = \frac{B + b^* q_1^{5e_1} \ldots q^{5e} p_1^{f_1} \ldots p^f \vartheta}{d(\vartheta)},$$

weil nun:

$$b = q_1^{e_1} \ldots q^e \omega_1 \mp b^*\vartheta = \frac{B q_1^{e_1} \ldots q^e}{d(\vartheta)} = \frac{B}{\pm b_1^*}$$

eine ganze rationale Zahl sein muß, so ist auch B durch b_1^* teilbar. Folglich kann man die Basiszahl ω_1 in der Gestalt:

$$\omega_1 = \frac{b + b^*\vartheta}{q_1^{e_1} \ldots q^e}$$

---

1) Die Resultate dieser Nummer sind als herrührend von Woronoj (siehe Fortschr. der Math., Bd. XXV, Jahrg. 1894) zitiert in der Dissertation von *W. L. Reid*, Tafel der Klassenanzahlen für kubische Zahlkörper. Gött. 1899.

zugrunde legen. Berücksichtigt man nun wieder, daß auch $x\omega_1 + y\vartheta$ eine ganze Zahl des Körpers ist, wenn x, y ganze rationale Zahlen sind, so folgert man weiter leicht, daß b^* als eine Zahl vorausgesetzt werden muß, welche in $q_1^{e_1}\ldots q^e$ aufgeht, oder welche nur irgend welche der Größen $q_1,\ldots,q$ als verschiedene Primfaktoren enthält; denn man kann x, y so bestimmen, daß $xb^* + yq_1^{e_1}\ldots q^e$ der größte gemeinsame Teiler von b^* und $q_1^{e_1}\ldots q^e$ ist.

Aus der Gleichung $q_1^{e_1}\ldots q^e\omega_1 - b^*\vartheta = b^*\,.\,\alpha = b$ folgt ferner, daß auch b durch b^* teilbar ist. Wenn man daher Zähler und Nenner von ω_1 durch b^* dividiert, erhält man schließlich für die Basiszahl ω_1 die Form:

$$\omega_1 = \frac{b_1 + \vartheta}{D},$$

bezw., wenn statt b_1 wieder b geschrieben wird:

$$\omega_1 = \frac{b + \vartheta}{D}. \tag{1}$$

Hier ist $D = q_1^{r_1}\ldots q^r$ eine ganze rationale Zahl, welche selbst, ebenso wie ihre Primfaktoren *mindestens* zur sechsten Potenz in $d(\vartheta)$ aufgeht. Falls $d(\vartheta)$ überhaupt keinen Primfaktor zur sechsten oder einer höheren Potenz enthält, so ist $D = 1$ und man kann $\omega_1 = \vartheta$ nehmen.

Für den nächsten Zweck empfiehlt es sich, $d(\vartheta)$ in der Form zu schreiben:

$$d(\vartheta) = \pm D^2\,.\,\overline{D},$$

und die Basiszahl ω_2 in der Form:

$$\omega_2 = \frac{C + C_1\vartheta + C_2\vartheta^2}{D^2\overline{D}}.$$

Dann ergeben sich für die Zahlen C, C_1 und C_2 nähere Bestimmungen durch Kombination der ganzen Zahl:

$$\omega_1^2 = \frac{b^2 + 2b\vartheta + \vartheta^2}{D^2},$$

mit ω_2. Indem man x, y als ganze rationale Zahlen geeignet wählt, kann nämlich zunächst $x\omega_1^2 + y\omega_2$ als ganze Zahl so bestimmt werden, daß der Koeffizient von ϑ^2 ein Teiler D_2 von $\overline{D}$ ist. Sei daher $\overline{D} = D_1 D_2$, dann ist man stets berechtigt der Zahl ω_2 die Gestalt:

$$\omega_2 = \frac{C + C_1\vartheta + D_2\vartheta^2}{D^2 D_1 D_2}$$

zu geben.

Nach der Definition der Körperbasis gibt es drei ganze rationale Zahlen u, v, w, welche die Gleichung erfüllen:

$$\omega_1^2 = u + v\omega_1 + w\omega_2. \tag{2}$$

Daraus folgen für u, v, w und die ganzen Zahlen C, C_1, D_2 usw. die Beziehungen:

$$w = D_1, \quad C_1 = D_2(+2b - vD), \quad C = D_2(b^2 - uD^2 - vbD), \tag{2a}$$

oder es sind C, C_1 durch D_2 teilbar:

$$C_1 = D_2 c_1, \quad C = D_2 c,$$

daher ergibt sich für ω_2 der noch einfachere Ausdruck:

$$\omega_2 = \frac{c + c_1\vartheta + \vartheta^2}{D^2 D_1}. \tag{3}$$

Die Wahl der Größen b, c, c_1 in den Gleichungen (1) und (3) ist noch in weiten Grenzen willkürlich. Um diese Wahl einzuschränken, benützen wir nun die Tatsache, daß ω_1, ω_2 ganze Zahlen sind und daß daher für b die Kongruenzen gelten müssen:

$$3b - a_1 \equiv 0, \ (D) \tag{4}$$

$$3b^2 - 2a_1 b + a_2 \equiv 0, \ (D^2) \tag{5}$$

$$b^3 - a_1 b^2 + a_2 b + a_3 \equiv 0, \ (D^3). \tag{6}$$

(a_1, a_2, a_3 sind die ganzzahligen Koeffizienten der Gleichung $G(x) = 0$, welche die Zahl ϑ definiert. Vergl. S. 244.)

Wegen der ersten dieser drei Kongruenzen darf man an Stelle von $\omega_1 = \frac{b + \vartheta}{D}$ auch jede der folgenden Zahlen als Basiszahl setzen, indem man gleichzeitig die Ausdrücke der Gleichung (2a) beachtet:

$$\frac{b + \vartheta}{D}; \quad \frac{a_1 - 2b + \vartheta}{D}; \quad \frac{a_1 - 2b + vD + \vartheta}{D} = \frac{a_1 - c_1 + \vartheta}{D}.$$

Es sei

$$\omega_1 = \frac{a_1 - c_1 + \vartheta}{D}. \tag{7}$$

Wählt man ferner in der Gleichung (2) anstatt der linken Seite ω_1^2 eine Zahl $\omega_1^2 - \frac{3b - a_1}{D} v - k$ und berücksichtigt weiter die Kongruenz (4), so läßt sich k derart bestimmen, daß man für u, v Werte bekommt, für welche:

$$c = c_1^2 - a_1 c_1 + a_2$$

wird. Schreibt man schließlich für c_1 den Buchstaben A, dann hat man jetzt die drei Basiszahlen in der folgenden Form, in der nur A, D, D_1 zu bestimmen übrig bleiben:

$$\omega = 1, \quad \omega_1 = \frac{-A + a_1 + \vartheta}{D}, \quad \omega_2 = \frac{A^2 - a_1 A + a_2 + A\vartheta + \vartheta^2}{D^2 D_1}. \tag{8}$$

Bei Annahme dieser Basis wird die Körperdiskriminante:

$$d = \frac{1}{D^6 D_1^2} d(\vartheta),$$

d. h. das Quadrat von D_1 muß in $d(\vartheta)$ aufgehen.

Als Bedingungen dafür, daß ω_1 eine ganze Zahl des Körpers ist, oder dafür, daß $\omega_1 + \omega_1' + \omega_1''$, $\omega_1\omega_1' + \omega_1'\omega_1'' + \omega_1''\omega_1$ und $\omega_1\omega_1'\omega_1''$ ganze rationale Zahlen sind, erhält man drei Kongruenzen. Dieselben gehen aus den Kongruenzen (4), (5), (6) hervor, wenn man darin b durch $-A + a_1$ ersetzt. Diese Kongruenzen werden aber teilweise umfaßt von denjenigen Kongruenzen, welche aussagen, daß ω_2 eine ganze Zahl des Körpers ist.

Damit $\omega_2 + \omega_2' + \omega_2''$ eine ganze rationale Zahl ist, muß:

$$3(A - a_1)^2 + 2a_1(A - a_1) + a_2 \equiv 0, \qquad (D^2 D_1)$$

sein. Durch eine einfache Rechnung ergibt sich ferner:

$$\omega_1\omega_2 = -\frac{G(A - a_1)}{D^3 D_1}$$

wobei $G(x) = x^3 + a_1x^2 + a_2x + a_3$ ist (entsprechend der Bezeichnung in Nr. 39), und daher wird

$$\omega_1\omega_1'\omega_1'' \cdot \omega_2\omega_2'\omega_2'' = -\frac{[G(A - a_1)]^3}{D^9 D_1^3}.$$

Weil andererseits nach Kongruenz (3):

$$\omega_1\omega_1'\omega_1'' = -\frac{G(A - a_1)}{D^3}$$

ist, so bleibt als Bedingung dafür, daß $\omega_2\omega_2'\omega_2''$ eine ganze rationale Zahl darstellt, die Kongruenz:

$$[G(A - a_1)]^2 \equiv 0, \qquad (D^6 D_1^3),$$

übrig. Diese Kongruenz ist dann und nur dann erfüllt, wenn:

$$G(A - a_1) = (A - a_1)^3 + a_1(A - a_1)^2 + a_2(A - a_1) + a_3 \equiv 0, \ (D^3 D_1^2)$$

ausfällt. Stellt man schließlich noch die Bedingung dafür auf, daß auch $\omega_2\omega_2' + \omega_2'\omega_2'' + \omega_2''\omega_2$ eine ganze rationale Zahl ist, so findet man:

$$\{3(A - a_1) + a_1\}\, G(A - a_1) \equiv 0, \qquad (D^4 D_1^2);$$

jedoch ist diese Kongruenz nicht neu, sie ist einfach das Produkt der Kongruenz (4), d. h.:

$$3(A - a_1) + a_1 \equiv 0, \quad (D),$$

und der zuletzt aufgestellten Kongruenz:

$$G(A - a_1) \equiv 0. \qquad (D^3 D_1^2).$$

Das Ergebnis aller bisherigen Betrachtungen läßt sich nun folgendermaßen zusammenfassen:

Die Basis eines Zahlkörpers $k(\vartheta)$, der durch eine Wurzel ϑ der Gleichung $G(x) = x^3 + a_1 x^2 + a_2 x + a_3 = 0$ bestimmt wird, ist:

$$\omega = 1, \quad \omega_1 = \frac{-(A-a_1)+\vartheta}{D}, \quad \omega_2 = \frac{(A-a_1)^2 + a_1(A-a_1) + a_2 + A\vartheta + \vartheta^2}{D^2 D_1},$$

wo mindestens D^6 und D_1^2 in $d(\vartheta)$ aufgehen und wo A, D, D_1 ganze rationale Zahlen sind, für welche die folgenden Kongruenzen bestehen, (d. h. in ganzen rationalen Zahlen lösbar sind):

$$3(A-a_1) + a_1 \equiv 0, \quad (D)$$

$$3(A-a_1)^2 + 2a_1(A-a_1) + a_2 \equiv 0, \quad (D^2 D_1)$$

$$(A-a_1)^3 + a_1(A-a_1)^2 + a_2(A-a_1) + a_3 \equiv 0, \quad (D^3 D_1^2).$$

Für den einen Faktor D in den Moduln dieser Kongruenzen könnte man noch weitere spezielle Angaben machen, doch will ich hier davon absehen und dies dem Leser überlassen.

Als einfachstes Beispiel für unsere Entwicklungen nehmen wir einen Körper $k(\vartheta)$, der durch eine Wurzel der Gleichung:

$$G(x) = x^3 + a_3 = 0$$

bestimmt ist.

Wir setzen voraus, daß a_3 *nicht* durch die dritte Potenz einer Primzahl teilbar sei, und es bezeichne N das Produkt aller Primzahlen, welche die Zahl a_3 zur zweiten Potenz enthält. Dann verbleiben für die Basis des Körpers $k(\vartheta)$ die folgenden Möglichkeiten:

1. Wenn $a_3 \equiv 0$, (3) ist, so ist:

$$\omega = 1, \quad \omega_1 = \vartheta, \quad \omega_2 = \frac{\vartheta^2}{N};$$

2. Wenn $a_3 \not\equiv 0$, (3), aber $a_3 \equiv \pm 2$, oder $a_3 \equiv \pm 4$, (9) ist, so wird wieder:

$$\omega = 1, \quad \omega_1 = \vartheta, \quad \omega_2 = \frac{\vartheta^2}{N};$$

3. Wenn $a_3 \equiv 1$, (9) ist, so ist:

$$\omega = 1, \quad \omega_1 = \vartheta, \quad \omega_2 = \frac{N - N\vartheta + \vartheta^2}{3N}, \text{ falls } N \equiv 1, (3),$$

und

$$\omega = 1, \quad \omega_1 = \vartheta, \quad \omega_2 = \frac{-N + N\vartheta + \vartheta^2}{3N}, \text{ falls } N \equiv -1, (3);$$

4. Wenn $a_3 \equiv -1$, (9) ist, so ist:

$$\omega = 1, \quad \omega_1 = \vartheta, \quad \omega_2 = \frac{N + N\vartheta + \vartheta^2}{3N}, \text{ falls } N \equiv 1 \ (3)$$

und

$$\omega = 1, \quad \omega_1 = \vartheta, \quad \omega_2 = \frac{-N - N\vartheta + \vartheta^2}{3N}, \text{ falls } N \equiv -1, (3).$$

In diesen Formeln ist $N = 1$ zu setzen, wenn die Zahl a_3 gar keine Primzahl zur Potenz 2 enthält.

Der Fall, daß a_3 auch Primzahlen zur dritten (und allgemein $(3\nu \pm 1)$ten) Potenz enthält, läßt sich auf den spezielleren Fall zurückführen. Ist z. B. $a_3' = p^3 . a_3$, so setze man $x = py$ und folglich $y^3 + a_3 = 0$ statt $x^3 + a_3' = 0$.

43. Die Ideale des Körpers $k(\vartheta)$ und ihre Zerlegung.

Die Division zweier ganzen Zahlen des Körpers ist wieder ganz ähnlich wie früher zu definieren. Eine ganze Zahl α heißt teilbar durch eine andere ganze Zahl β, wenn man eine ganze Zahl γ des Körpers so bestimmen kann, daß:

$$\alpha = \beta . \gamma$$

ist. Sieht man von solchen ganzen Faktoren der Zahl α ab, welche zugleich in 1 aufgehen, und die man kurz Einheiten nennen kann, so sieht man durch Übergang zu den Normen, daß eine Zahl α jedenfalls nur eine endliche Anzahl von verschiedenen Faktoren enthalten kann. Denkt man sich aber eine Zerlegung von α so weit ausgeführt, daß keiner der Faktoren mehr zerlegbar ist, so stößt man auch für die kubischen Zahlen auf dieselbe Schwierigkeit wie im Gebiet des quadratischen Zahlkörpers: die Zerlegung einer ganzen Zahl des Körpers in unzerlegbare Faktoren ist im allgemeinen nicht eindeutig.

Um wieder zu einfachen Zerlegungsgesetzen für den Körper zu kommen, führt man wieder *Ideale* ein, wie beim quadratischen Körper, und man betrachtet den Körper als Inbegriff seiner Zahlen und Ideale. Wir brauchen nur die Betrachtungen von Abschn. II, Nr. 9, S. 37 ff. zu erweitern.

Definition. Ein Ideal $\mathfrak{j}$ heißt der Inbegriff (das System) von unbegrenzt vielen ganzen Zahlen des Körpers $k(\vartheta)$:

$$\mathfrak{j} = (\alpha, \beta, \gamma, \ldots),$$

mit der Eigenschaft, daß jede lineare Kombination $\lambda_1\alpha + \lambda_2\beta + \lambda_3\gamma + \cdots$, der Zahlen $\alpha, \beta, \gamma, \ldots$ mit irgend welchen ganzen Zahlen $\lambda_1, \lambda_2, \lambda_3, \ldots$ des Körpers, wiederum dem System $\mathfrak{j}$ angehört.

An diese Definition schließen sich sogleich einige einfache Bemerkungen und Folgerungen an:

1. Jedes Ideal enthält die Zahl 0.

2. Ein Ideal enthält außer einer Zahl α immer auch die ganze rationale Zahl $n(\alpha)$, da $\alpha'\alpha''$ eine ganze Zahl des Körpers $k(\vartheta)$ is

Es enthält also jedes Ideal auch unendlich viele ganze rationale Zahlen.

3. Wenn ein Ideal eine Zahl α enthält, die in 1 aufgeht, so enthält es auch die Zahl 1, und das Ideal ist ein *Einheitsideal*.

4. Wenn in einem Ideal alle Zahlen $\alpha, \beta, \gamma \ldots$ durch eine dem Ideal angehörige Zahl des Ideals, z. B. durch α, teilbar sind, so heißt dasselbe ein *Hauptideal* und wird einfach geschrieben:

$$\mathfrak{j} = (\alpha)$$

Für die Ideale des quadratischen Zahlkörpers haben wir den Begriff einer Basis aufgestellt und den Nachweis für die Existenz einer Basis geführt. Unter Benutzung derselben Schlüsse und derjenigen, die zum Nachweis der Existenz einer Basis des Körpers führten, kann man auch für den erweiterten Begriff folgenden Satz beweisen:

Satz. *In jedem Ideal $\mathfrak{j}$ des Körpers $k(\vartheta)$ kann man auf unendlich viele Weisen drei Zahlen $\iota_1, \iota_2, \iota_3$ so auswählen, daß jede andere Zahl des Ideals in der Gestalt darstellbar ist:*

$$x\iota_1 + y\iota_2 + z\iota_3,$$

wo x, y, z ganze rationale Zahlen sind.

Die drei Zahlen $\iota_1, \iota_2, \iota_3$ bilden eine *Basis des Ideals*.

Man kann insbesondere wieder eine Normalbasis im Ideal so wählen, daß:

$$\iota_1 = i, \qquad \iota_2 = i_1 + i_1^{(1)}\omega_1, \qquad \iota_3 = i_2 + i_2^{(1)}\omega_1 + i_2^{(2)}\omega_2$$

wird. Man schreibt ein Ideal, das durch seine Basis gegeben ist, am bequemsten in der folgenden Weise:

$$\mathfrak{j} = (\iota_1, \iota_2, \iota_3)$$

oder

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3) \text{ usw.}$$

Wählt man die ganzen Zahlen a_{rs} so, daß $(a_{11}a_{22}a_{33}) = \pm 1$ wird, und dies kann auf unendlich viele Weisen geschehen, so bildet auch das Zahlentripel:

$$\iota_r^* = a_{r1}\iota_1 + a_{r2}\iota_2 + a_{r3}\iota_3 \;(r = 1, 2, 3),$$

wieder eine Basis des Ideals $\mathfrak{j}$, *es gibt daher wiederum unendlich viele Zahlentripel im Ideal, die eine Basis des Ideals bilden.*

Überall nun, wo es sich um Teilbarkeitssätze für den Körper handelt, treten die Ideale an die Stelle der ganzen Zahlen des Körpers. Die Multiplikation und die Division der ganzen Zahlen, jedoch nicht die Addition, lassen sich auf die Ideale übertragen, und zwar gelten wieder die folgenden Definitionen:

Definition. Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale des Körpers $k(\vartheta)$, etwa:

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \ldots), \qquad \mathfrak{b} = (\beta_1, \beta_2, \beta_3, \ldots),$$

so versteht man unter dem Produkt der beiden Ideale $\mathfrak{a}$, $\mathfrak{b}$ dasjenige Ideal $\mathfrak{c}$, welches aus dem System der Zahlen besteht, das man erhält, wenn man jede Zahl des Ideals $\mathfrak{a}$ mit jeder Zahl des Ideals $\mathfrak{b}$ multipliziert und außerdem noch die linearen Kombinationen dieser Produkte mit beliebigen ganzen Zahlen $\lambda_1, \lambda_2, \ldots$ des Körpers $k(\vartheta)$ hinzufügt.

Und umgekehrt:

Ein Ideal $\mathfrak{c}$ heißt *teilbar* durch ein Ideal $\mathfrak{a}$, wenn man ein Ideal $\mathfrak{b}$ des Körpers angeben kann so, daß $\mathfrak{c} = \mathfrak{a} . \mathfrak{b}$ ist.

Eine unmittelbare Folgerung dieser Definition ist offenbar die Tatsache: Wenn ein Ideal $\mathfrak{c}$ durch ein Ideal $\mathfrak{a}$ teilbar ist, so ist jede Zahl des Ideals $\mathfrak{c}$ auch zugleich eine Zahl des Ideals $\mathfrak{a}$.

Ein von (1) verschiedenes Ideal, welches nur durch sich selbst und Einheitsideale teilbar ist, soll wieder *Primideal* genannt werden. Man muß in der Körpertheorie den Ausdruck Primzahl vermeiden, da Zweideutigkeiten entstehen könnten. Es kann ja sehr wohl eine ganze Zahl des Körpers als Zahl unzerlegbar sein, während das durch die Zahl bestimmte Hauptideal in weitere Faktoren zerfällt.

Definition. Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen äquivalent, wenn im Körper $k(\vartheta)$ zwei ganze Zahlen α, β existieren, so daß

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha}{\beta}$$

wird.

Wir dürfen die Formulierung der Fundamentalsätze über die Äquivalenz (z. B.: Sind zwei Ideale einem dritten äquivalent, so sind sie es unter sich; u. A., s. Satz 1, 2 Nr. 16, S. 72) dem Leser überlassen.

Den Begriff der Äquivalenz benützt man wieder zur Einteilung der Ideale in Klassen: *Alle äquivalenten Ideale bilden eine Klasse.*

Nach diesen Vorbereitungen kann man gleich zum Fundamentalsatz über die eindeutige Zerlegbarkeit der Ideale übergehen. Ich folge dabei der zweiten von Herrn Hurwitz gegebenen Begründung der Idealtheorie.[1]).

---

1) A. Hurwitz. Nachr. von der kgl. Ges. d. Wissensch. zu Gött. 1895. S. 323. Bei dieser Begründung der Theorie der Ideale ist der Satz über die eindeutige Zerlegung der Ideale in Primfaktoren eine Folge der Endlichkeit der Klassenanzahl. Es ist dies eine äußerst merkwürdige Tatsache. Eine ganz gleiche Begründung, nur mit anderen Mitteln, hat zur selben Zeit P. Furtwängler entwickelt. Ibid. S. 381.

Hilfssatz. *Eine ganze Zahl α des Körpers mit endlicher Norm $\pm a$ kann nur in einer* ***endlichen*** *Anzahl voneinander verschiedener Ideale auftreten.*

Beweis. Es sei

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \ldots \alpha \ldots),$$

und a eine rationale Zahl des Ideals. Stellt dann $\omega_1 = 1$, ω_2, ω_3 eine Basis des Körpers dar, und ist $\iota_1 = i$, $\iota_2 = i_1 + i_1^{(1)}\omega_2$, $\iota_3 = i_2 + i_2^{(1)}\omega_2 + i_2^{(2)}\omega_3$ die Normalbasis des Ideals, so sind $i, i_1, \ldots i_2^{(2)}$ ganze rationale Zahlen aus dem vollen System der kleinsten Reste nach dem Modul a. Da nämlich mit a auch zugleich $a\omega_1$, $a\omega_2$, $a\omega_3$ dem Ideal $\mathfrak{a}$ angehören, so sind i, $i_1^{(1)}$, $i_2^{(2)}$ Teiler der Zahl a. Weil ferner die Zahl $|i|$ nicht kleiner ist als die absoluten Beträge der übrigen Koeffizienten i_1 bis $i_2^{(2)}$, so ist die Behauptung offenbar richtig.

Indem man an Stelle der Koeffizienten i bis $i_2^{(2)}$ alle möglichen Kombinationen der Zahlen des kleinsten Restsystems nach a setzt, erhält man eine endliche Anzahl verschiedener Systeme von Basiszahlen und verschiedener Ideale $\mathfrak{a}$.

Dieser Hilfssatz läßt ohne weiteres die Richtigkeit der folgenden Behauptung erkennen:

Satz. *Ein Ideal kann stets nur eine endliche Anzahl verschiedener Idealteiler besitzen.*

Man braucht außer dem vorausgehenden Hilfssatz nur die Bemerkung zu berücksichtigen, daß jede Zahl des Dividendus auch im Divisor vorkommen muß.

Die Grundlage des Beweises für den Fundamentalsatz bildet aber nun der folgende zweite Hilfssatz:

Hilfssatz. *Die Anzahl der voneinander verschiedenen Idealklassen des Körpers $k(\vartheta)$ ist eine endliche Zahl (jedes beliebige Ideal des Körpers ist mindestens einem Ideal äquivalent, das eine endliche rationale ganze Zahl enthält, deren Wert nur von der Diskriminante des Körpers abhängig ist).*

Beweis. Beim Beweis des Satzes ist es notwendig, die reellen und imaginären Körper zu unterscheiden.

Es sei zunächst $k(\vartheta)$ ein reeller Körper und

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3)$$

ein beliebiges Ideal mit der Basis:

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + a_{i3}\omega_3 \quad (\text{für } i = 1, 2, 3).$$

Denkt man sich dann die Normen von allen Zahlen des Ideals $\mathfrak{a}$ gebildet, so ergeben die absoluten Beträge dieser Normen eine Zahlen-

reihe, in welcher eine Zahl die kleinste ist; es möge ι eine Zahl des Ideals sein, welcher diese kleinste Norm zukommt. Nun behaupten wir: man kann stets eine endliche ganze rationale, nur von der Diskriminante d des Körpers abhängige Zahl A angeben, von der Beschaffenheit, daß $A\alpha$ durch ι teilbar ist, wenn unter α eine *beliebige* Zahl des Ideals verstanden wird.

In der Tat, bezeichnet α_i eine beliebige der drei Basiszahlen, so kann man nach dem Satz von Minkowski, S. 65, vier ganze rationale Zahlen u, x, y, z, die nicht sämtlich Null sind, so bestimmen, daß die vier Bedingungen erfüllt werden:

$$\begin{aligned}
&|\alpha_i u + \iota\omega_1 x + \iota\omega_2 y + \iota\omega_3 z| \leqq \varkappa_1\\
&|\alpha_i' u + \iota'\omega_1' x + \iota'\omega_2' y + \iota'\omega_3' z| \leqq \varkappa_2\\
&|\alpha_i'' u + \iota''\omega_1'' x + \iota''\omega_2'' y + \iota''\omega_3'' z| \leqq \varkappa_3\\
&\left|\frac{\pm\alpha_i u}{\sqrt{d}}\right| \leqq \varkappa_4.
\end{aligned}$$

Hierbei bezeichnen $\varkappa_1, \varkappa_2, \varkappa_3, \varkappa_4$ vier positive Größen, deren Produkt gleich der positiv zu wählenden Determinante der vier Formen ist:

$$\varkappa_1\varkappa_2\varkappa_3\varkappa_4 = \frac{\pm\alpha_i}{\sqrt{d}}\, n(\iota)\begin{vmatrix}\omega_1 & \omega_2 & \omega_3\\ \omega_1' & \omega_2' & \omega_3'\\ \omega_1'' & \omega_2'' & \omega_3''\end{vmatrix} = \pm\alpha_i \,.\, n(\iota).$$

Wählt man, was erlaubt ist, $\varkappa_4 = 2|\alpha_i|$, also $|u| \leqq |2\sqrt{d}|$, und setzt nun:

$$\beta = \alpha_i u + \iota(\omega_1 x + \omega_2 y + \omega_3 z),$$

so ist β eine ganze Zahl, für welche:

$$|n(\beta)| \leqq \varkappa_1\varkappa_2\varkappa_3 \quad \text{und wegen} \quad \varkappa_1\varkappa_2\varkappa_3 = \tfrac{1}{2}|n(\iota)|,$$

somit:

$$|n(\beta)| \leqq \tfrac{1}{2}|n(\iota)|$$

ausfällt. β ist eine Zahl des Ideals $\mathfrak{a}$, denn sie stellt eine lineare Kombination der Idealzahlen α_i und ι mit ganzen Zahlen des Körpers dar, weil u und $\omega_1 x + \omega_2 y + \omega_3 z = \lambda$ ganze Zahlen sind. Ferner kann u nicht gleich Null werden, denn λ ist von Null verschieden und man erhielte die Ungleichung:

$$|n(\beta)| = |n(\iota)\, n(\omega_1 x + \omega_2 y + \omega_3 z)| \leqq \tfrac{1}{2}|n(\iota)| \quad \text{oder} \quad |n(\lambda)| \leqq \tfrac{1}{2};$$

d. h. $n(\omega_1 x + \omega_2 y + \omega_3 z)$ wäre überhaupt keine *ganze* rationale Zahl. Diese Konsequenz widerspricht dem Satz über die ganzzahligen Funktionen ganzer algebraischer Zahlen, nach dem $|n(\lambda)| \geqq 1$ ist.

Nun ist aber ι eine Zahl des Ideals mit dem kleinstmöglichen Wert der Norm $|n(\iota)|$, also muß notwendig $n(\beta) = 0$, folglich auch $\beta = 0$ sein. Die Gleichung $\beta = 0$, bezw.:

$$\alpha_i u + \lambda\iota = 0,$$

läßt sich aber so in Worten formulieren: *Für jede der Zahlen* α_i *läßt sich eine ganze rationale Zahl* $|u| < |2\sqrt{d}|$ *so bestimmen, daß* $\alpha_i u$ *durch* ι *teilbar ist.*

Dieser Faktor u braucht nicht derselbe zu sein für alle drei Zahlen α_i und ist sicher nicht derselbe für verschiedene Ideale $\mathfrak{a}$, $\mathfrak{a}_1$ usw.; bezeichnet aber A das Produkt aller positiven ganzen rationalen Zahlen, die kleiner sind als $2|\sqrt{d}|$, dann sind sicher die Produkte aller drei Basiszahlen α_1, α_2, α_3 mit A, d. h. $A\alpha_i$, durch ι teilbar, und folglich ist auch für eine ganz beliebige Zahl α des Ideals das Produkt $A \,.\, \alpha$ durch ι teilbar.

Unter Berücksichtigung der Bedeutung der Zahlen A, ι gilt daher jetzt folgende Idealgleichung:

$$(A)\mathfrak{a} = (A\alpha_1,\ A\alpha_2,\ A\alpha_3,\ A\iota, \ldots) = \iota(\lambda_1,\ \lambda_2,\ \lambda_3,\ A, \ldots)$$

oder

$$(A)\mathfrak{a} = (\iota)\,.\,\mathfrak{b}; \qquad \mathfrak{a} \sim \mathfrak{b}.$$

D. h.: ein beliebiges Ideal $\mathfrak{a}$ des Körpers ist stets äquivalent einem anderen Ideal $\mathfrak{b}$, welches die Zahl A enthält. Dabei ist A eine *endliche* ganze rationale Zahl, wenn d endlich ist. Nach dem zuerst angeführten Hilfssatz existiert nur eine endliche Anzahl verschiedener Ideale $\mathfrak{b}$, welche die endliche Zahl A enthalten. Folglich muß es möglich sein, im Körper eine endliche Anzahl h von Idealen

$$\mathfrak{b}_1,\ \mathfrak{b}_2, \ldots, \mathfrak{b}_h$$

derart zu bestimmen, daß jedes *beliebige* Ideal des Körpers einem und nur einem einzigen dieser h Ideale äquivalent ist. Oder:

Die Klassenanzahl h *eines reellen Körpers* $k(\vartheta)$ *ist stets eine endliche Zahl.*

Es sei zweitens $k(\vartheta)$ ein imaginärer Körper, und $\mathfrak{a}$, α_i, α, ι haben dieselbe Bedeutung wie vorhin im Falle des reellen Körpers, aber α_i, α seien jetzt *komplexe* Zahlen. Dann sucht man wieder in dem Ideal $\mathfrak{a}$ eine ganze Zahl:

$$\beta = \alpha_i u + \iota(\omega_1 x + \omega_2 y + \omega_3 z)$$

derart, daß $|n(\beta)| < |n(\iota)|$, oder $\beta = 0$ wird. Wenn α' die zu der beliebigen komplexen Zahl α konjugierte, ebenfalls komplexe Zahl und α'' die zu α konjugierte reelle Zahl bezeichnet, so erreicht man

das Ziel in der folgenden Weise: Man wendet den Satz von Minkowski auf vier lineare Formen:

$$\frac{1}{\sqrt{2}}(\beta+\beta'), \qquad \frac{1}{\sqrt{-2}}(\beta-\beta'), \qquad \beta'', \qquad \pm\frac{|\alpha_i|u}{|\sqrt{d}|}$$

in der Art an, daß

$$\begin{aligned} \left|\frac{1}{\sqrt{2}}(\beta+\beta')\right| &\leqq \varkappa_1 \\ \left|\frac{1}{\sqrt{-1}\sqrt{2}}(\beta-\beta')\right| &\leqq \varkappa_1 \\ |\beta''| &\leqq \varkappa_3 \\ \left|\frac{\alpha_i u}{\sqrt{d}}\right| &\leqq \varkappa_4, \end{aligned}$$

wird, wo $\beta=\alpha_i u+\iota\omega_1 x+\iota\omega_2 y+\iota\omega_3 z$ und $\varkappa_1^2\varkappa_3\varkappa_4=2\,|\alpha_i n(\iota)|$ zu setzen ist.

Indem man nun $\varkappa_4=4\,|\alpha_i|$ setzt und im übrigen wieder genau so verfährt wie oben, erhält man:

$$\varkappa_1^2\varkappa_3=\tfrac{1}{2}\,|n(\iota)|$$

und

$$\begin{aligned} |n(\beta)| &= \left|\left\{\left(\frac{1}{2}(\beta+\beta')\right)^2+\left(\frac{1}{2\sqrt{-1}}(\beta-\beta')\right)^2\right\}\beta''\right| \\ &= \left\{\left(\frac{\varkappa_1}{\sqrt{2}}\right)^2+\left(\frac{\varkappa_1}{\sqrt{2}}\right)^2\right\}\varkappa_3 \\ &= \varkappa_1^2\varkappa_3<\tfrac{1}{2}\,|n(\iota)|\,. \end{aligned}$$

Daraus lassen sich dieselben Folgerungen ableiten wie oben, und wir dürfen also den allgemein gültigen Satz aussprechen:

Die Klassenanzahl h eines jeden Körpers $k(\vartheta)$ ist eine endliche Zahl.

Aus diesem zweiten Hilfssatz ergibt sich nun in der einfachsten Weise der Beweis des folgenden Satzes, der dem Satz über die eindeutige Zerlegung eines Ideals in Faktoren gleichwertig ist.

Satz. *Ist $\mathfrak{a}$ ein beliebiges Nichthauptideal des Körpers, dann kann man stets ein Ideal $\mathfrak{b}$ angeben, welches ebenfalls nicht Hauptideal ist, von der Beschaffenheit, daß das Produkt $\mathfrak{a}\,.\,\mathfrak{b}$ ein Hauptideal wird.*

Beweis. Sei $\mathfrak{a}$ ein Nichthauptideal, so bilde man die aufeinanderfolgenden Potenzen:

$$\mathfrak{a},\ \mathfrak{a}^2,\ \mathfrak{a}^3,\ldots$$

Nach dem zweiten Hilfssatz verteilen sich diese Potenzen auf eine endliche Anzahl Klassen, und man darf als allgemeinsten Fall an-

nehmen, daß $\mathfrak{a}^{m+h_1}$ die erste Potenz ist, welche einem früheren Gliede der Reihe, nämlich $\mathfrak{a}^m$, äquivalent ist. Es sei also:

$$\mathfrak{a}^{m+h_1} \sim \mathfrak{a}^m,$$

oder

$$(\alpha)\mathfrak{a}^{m+h_1} = (\beta)\mathfrak{a}^m,$$

oder endlich:

$$\mathfrak{a}^{m+h_1} = (\lambda)\mathfrak{a}^m, \tag{1}$$

wo α, β ganze Zahlen des Körpers $k(\vartheta)$ bedeuten. Dann ist zu zeigen, daß $\mathfrak{a}^{h_1}$ ein Hauptideal gleich (λ) ist. Dazu soll zunächst von der durch Gleichung (1) definierten Zahl λ nachgewiesen werden, daß sie eine *ganze* Zahl des Körpers ist.

Zu diesem Zwecke bemerke man zuerst, daß alle Zahlen des Ideals $\mathfrak{a}^{m+h_1}$ zugleich Zahlen des Ideals $\mathfrak{a}^m$ sind, indem $\mathfrak{a}^{m+h_1}$ aus $\mathfrak{a}^m$ durch Multiplikation mit $\mathfrak{a}^{h_1}$ hervorgeht. Bezeichnet dann $\alpha_1, \alpha_2, \alpha_3$ eine Basis des Ideals $\mathfrak{a}^m$, so ist $\lambda\alpha_1$ eine ganze Zahl, weil sie dem Ideal $\mathfrak{a}^{m+h_1}$ angehört. Als Zahl des Ideals $\mathfrak{a}^m$ läßt sich $\lambda\alpha_1$ durch folgende lineare Kombination mit ganzzahligen rationalen Zahlenkoeffizienten darstellen:

$$\lambda\alpha_1 = x_1\alpha_1 + y_1\alpha_2 + z_1\alpha_3;$$

ebenso ist:

$$\lambda\alpha_2 = x_2\alpha_1 + y_2\alpha_2 + z_2\alpha_3,$$

$$\lambda\alpha_3 = x_3\alpha_1 + y_3\alpha_2 + z_3\alpha_3.$$

Durch Elimination von α_1, α_2, α_3 aus diesen drei Gleichungen erhält man für λ die Bedingung:

$$\begin{vmatrix} x_1 - \lambda & y_1 & z_1 \\ x_2 & y_2 - \lambda & z_2 \\ x_3 & y_3 & z_3 - \lambda \end{vmatrix} = 0.$$

Weil hier die x_i, y_i, z_i lauter ganze rationale Zahlen bezeichnen, so erfüllt λ eine Gleichung dritten Grades, in welcher alle Koeffizienten ganze Zahlen sind und gleichzeitig der Koeffizient des höchsten Gliedes gleich 1 ist. λ ist also eine ganze algebraische Zahl.

Wenn jetzt ferner β eine beliebige Zahl des Ideals $\mathfrak{a}^{h_1}$ ist, so ist $\beta\alpha_1, \beta\alpha_2, \beta\alpha_3$ jedesmal eine Zahl des Idealprodukts $(\lambda)\mathfrak{a}^m$. Indem man jene 3 Zahlen durch die Basis $\lambda\alpha_1, \lambda\alpha_2, \lambda\alpha_3$ von $(\lambda)\mathfrak{a}^m$ darstellt und $\alpha_1, \alpha_2, \alpha_3$ wieder wie vorhin aus den drei Gleichungen eliminiert, erhält man für $\frac{\beta}{\lambda}$ eine Gleichung dritten Grades mit ganzzahligen Koeffizienten, woraus hervorgeht, daß $\frac{\beta}{\lambda}$ eine ganze Zahl des Körpers ist.

Jede Zahl aus $\mathfrak{a}^{h_1}$ ist also durch λ teilbar, somit auch $\mathfrak{a}^{h_1}$ selbst, oder es ist $\mathfrak{a}^{h_1} = (\lambda)\mathfrak{j}$. Als Resultat erhält man daher, daß:

$$\mathfrak{a}^{m+h_1} = \mathfrak{a}^m \mathfrak{a}^{h_1} = \mathfrak{a}^m (\lambda)\mathfrak{j}$$

ist, wo $\mathfrak{j}$ ein Ideal des Körpers bedeutet. Die Idealgleichung:

$$\mathfrak{a}^{m+h_1} = (\lambda)\mathfrak{a}^m$$

ergibt ferner:

$$\mathfrak{a}^m (\lambda)\mathfrak{j} = (\lambda)\mathfrak{a}^m,$$

oder da mit λ dividiert werden darf:

$$\mathfrak{a}^m \mathfrak{j} = \mathfrak{a}^m,$$

und aus dieser Gleichung folgt schließlich, daß das Ideal $\mathfrak{j}$ auch die Zahl[1] 1 enthält, sonach daß $\mathfrak{a}^{h_1} = (\lambda)$ ein Hauptideal ist.

Aus der Gleichung:

$$\mathfrak{a}^{h_1} = (\lambda) \sim 1,$$

folgt jetzt ferner:

$$\mathfrak{a}^{1+h_1} = \mathfrak{a} \cdot \mathfrak{a}^{h_1} \sim \mathfrak{a}, \quad \mathfrak{a}^{2+h_1} \sim \mathfrak{a}^2 \quad \text{usw.};$$

es ist m. a. Worten in der ursprünglichen Annahme $m = 1$ zu setzen, und nach Voraussetzung müssen notwendig die Ideale $\mathfrak{a}, \mathfrak{a}^2, \ldots \mathfrak{a}^{h_1-1}$ alle untereinander inäquivalent sein.

Ist nun $\mathfrak{a}$ ein beliebiges Nichthauptideal des Körpers, so ist $\mathfrak{b} = \mathfrak{a}^{h_1-1}$ ein anderes Nichthauptideal von der gewünschten Eigenschaft, daß $\mathfrak{a}\mathfrak{b}$ ein Hauptideal wird.

Auf Grund dieses Satzes beweist man jetzt, wie wohl nicht nochmals näher auszuführen ist, der Reihe nach folgende Tatsachen:

Satz. *Sind* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *drei von Null verschiedene Ideale, welche der Gleichung genügen:* $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$, *so ist auch* $\mathfrak{a} = \mathfrak{b}$.

Ferner gilt die Umkehrung eines oben ausgesprochenen Satzes:

---

1) In der Tat ist jede Zahl des Produkts $\mathfrak{a}^m\mathfrak{j}$ eine Zahl in $\mathfrak{a}^m$, und umgekehrt. Schreibt man die Basis des Ideals $\mathfrak{j}$ mit $\iota_1, \iota_2, \iota_3$, so kann man offenbar alle Zahlen des Ideals $\mathfrak{a}^m$ darstellen in der Form:

$$\lambda_1 \alpha_1 (x_1 \iota_1 + y_1 \iota_2 + z_1 \iota_3) + \lambda_2 \alpha_2 (x_2 \iota_1 + y_2 \iota_2 + z_2 \iota_3) + \lambda_3 \alpha_3 (x_3 \iota_1 + y_3 \iota_2 + z_3 \iota_3),$$

wo $\lambda_1, \lambda_2, \lambda_3$ ganz beliebige Zahlen des Körpers $k(\vartheta)$ und die x_i, y_i, z_i ganze rationale Zahlen sind. Da andererseits durch

$$u_1 \alpha_1 + u_2 \alpha_2 + u_3 \alpha_3$$

alle Zahlen in $\mathfrak{a}^m$ darstellbar sind, so kann man die Zahlen λ_i, x_i, y_i, z_i stets so bestimmen, daß

$$\lambda_i (x_i \iota_1 + y_i \iota_2 + z_i \iota_3)$$

für $i = 1, 2, 3$ drei zueinander prime rationale Zahlen darstellen, die dann dem Ideal $\mathfrak{j}$ angehören und aus denen durch geeignete lineare Kombination mit ganzen rationalen Zahlen sich die Einheit bilden läßt, was zu beweisen war.

Satz. *Wenn alle Zahlen eines Ideals* $\mathfrak{a}$ *in einem Ideal* $\mathfrak{b}$ *vorkommen, so ist* $\mathfrak{a}$ *teilbar durch* $\mathfrak{b}$.

Nach diesem Satz erhalten wir wieder als *größten gemeinsamen Teiler zweier Ideale* $\mathfrak{a}$, $\mathfrak{b}$ dasjenige Ideal, das durch Vereinigung aller Zahlen aus $\mathfrak{a}$ *und* $\mathfrak{b}$ zu einem Ideal entsteht.

Schließlich:

Satz. *Falls das Produkt* $\mathfrak{a}\mathfrak{b}$ *zweier Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *durch ein Primideal* $\mathfrak{p}$ *teilbar ist, und falls etwa* $\mathfrak{a}$ *nicht teilbar durch* $\mathfrak{p}$ *ist, so ist sicher* $\mathfrak{b}$ *teilbar durch* $\mathfrak{p}$. Oder: *Wenn ein Primideal* $\mathfrak{p}$ *in dem Produkt* $\mathfrak{a}\mathfrak{b}$ *aufgeht, so muß* $\mathfrak{p}$ *mindestens in einem der Faktoren* $\mathfrak{a}$ *oder* $\mathfrak{b}$ *aufgehen.*

Diese Sätze zusammen sind aber identisch mit dem Satze, daß jedes Ideal nur auf eine einzige Weise in Primideale zerlegbar ist.

Als eine fundamentale Folgerung aus dem Satze von der eindeutigen Zerlegbarkeit der Ideale ist hervorzuheben, daß jedes Primideal $\mathfrak{p}$ des Körpers in einer rationalen Primzahl p aufgehen muß.

In der Tat kann man zu einem gegebenen Primideal $\mathfrak{p}$ einen Idealfaktor $\mathfrak{j}$ bestimmen, so daß $\mathfrak{p}\cdot\mathfrak{j}=(\alpha)$ ein Hauptideal wird. Da nun $\alpha\alpha'\alpha''=a$ eine ganze rationale Zahl ist, so geht $\mathfrak{p}$ in a und daher auch in einem (und nur einem) bestimmten rationalen Primfaktor p von a auf.

Nachdem aber alle diese Sätze bewiesen sind, folgt aus der schon in Nr. 16, S. 77 benutzten Schlußweise, daß die oben benützte Zahl h_1, für welche $\mathfrak{a}^{h_1}$ ein Hauptideal war, stets ein Teiler der Klassenanzahl h des Körpers sein muß. Man hat in der Tat nur nötig, die sämtlichen Klassen in Reihen mit je h_1 Klassen anzuschreiben.

Die Reihe $\mathfrak{a}, \mathfrak{a}^2, \ldots \mathfrak{a}^{h_1}$ heißt zuweilen auch *die Periode des Ideals* $\mathfrak{a}$.

Für die numerische Berechnung von Idealen bestimmter Zahlkörper, wobei natürlich nicht unendlich viele Zahlen geschrieben werden können, ist insbesondere der folgende Satz von der größten Bedeutung:

Satz. *In jedem Nichthauptideal* $\mathfrak{a}$ *des Körpers* $k(\vartheta)$ *kann man stets zwei Zahlen* α *und* α_1 *angeben, als deren größter gemeinsamer Teiler sich* $\mathfrak{a}$ *darstellen läßt, so daß* $\mathfrak{a}=(\alpha,\alpha_1)$ *gesetzt werden kann.*

Beweis. α sei eine Zahl des Ideals $\mathfrak{a}$, von der Beschaffenheit, daß:

$$(\alpha)=\mathfrak{a}\cdot\mathfrak{b}$$

wird, und $\mathfrak{b}$ prim zu $\mathfrak{a}$ ist. Dann wähle man in $\mathfrak{a}$ eine zweite Zahl α_1, welche nicht in $\mathfrak{b}$ vorkommt, für welche

$$(\alpha_1) = \mathfrak{a} \cdot \mathfrak{c},$$

ist. Nun sind $\mathfrak{b}$ und $\mathfrak{c}$ notwendig prim zueinander, und es ist $\mathfrak{a}$ der größte gemeinsame Teiler von α und α_1, d. h.

$$\mathfrak{a} = (\alpha, \alpha_1).$$

Weil nämlich $\mathfrak{b}$ prim ist zu $\mathfrak{c}$, so kann man in $\mathfrak{b}$ eine Zahl β und in $\mathfrak{c}$ eine Zahl γ so angeben, daß $\beta + \gamma = 1$ wird. Es lassen sich daher durch die Form $\lambda\alpha + \lambda_1\alpha_1$ alle Zahlen α_i aus $\mathfrak{a}$ darstellen. In der Tat ist stets: $\alpha_i = \alpha_i\beta + \alpha_i\gamma = \lambda\alpha + \lambda_1\alpha_1$.

44. Die Norm eines Ideals.

Es liegt nahe, den Begriff der Kongruenz zu erweitern auf den Fall, wo der Modul ein beliebiges Ideal ist. Man kann sagen, daß eine ganze Zahl α des Körpers $k(\vartheta)$ kongruent Null nach dem Ideal-Modul $\mathfrak{j}$ ist, oder:

$$\alpha \equiv 0, (\mathfrak{j}),$$

wenn die Zahl α im Ideal $\mathfrak{j}$ vorkommt. D. h. wenn $\alpha \equiv 0, (\mathfrak{j})$ ist, so ist (α) durch $\mathfrak{j}$ teilbar. Zwei beliebige ganze Zahlen des Körpers α, β heißen mod $(\mathfrak{j})$ kongruent, in Zeichen:

$$\alpha \equiv \beta, (\mathfrak{j}),$$

wenn ihre Differenz dem Ideal $\mathfrak{j}$ angehört (vgl. S. 45).

Aus dieser Definition folgt dann wieder, daß zwei ganze Zahlen des Körpers, welche einer dritten ganzen Zahl mod $(\mathfrak{j})$ kongruent sind, auch untereinander kongruent sein müssen. Man kann die Gesamtheit aller ganzen Zahlen mod $(\mathfrak{j})$ in Klassen einteilen, indem man alle Zahlen zu einer Klasse rechnet, welche einer bestimmten Zahl mod $(\mathfrak{j})$ kongruent sind. Jede Zahl des Körpers gehört einer Klasse an, und jede Zahl einer Klasse bestimmt immer wieder nur dieselbe Klasse.

Wählt man aus jeder dieser endlich vielen Klassen irgend eine Zahl aus, so erhält man ein System von ganzen Zahlen, das als *vollständiges Restsystem* nach dem Modul $\mathfrak{j}$ bezeichnet wird. Jede Zahl des Körpers ist einer einzigen Zahl des Restsystems mod $(\mathfrak{j})$ kongruent.

Die Wahl der Zahlen eines vollständigen Restsystems ist vorerst noch in weiten Grenzen willkürlich; wohl kann man aber nach der *Anzahl* der Zahlen fragen, welche in einem vollständigen Restsystem mod $(\mathfrak{j})$ enthalten sind. Diese nun zu bestimmende Zahl heißt die *Norm* des Ideals $\mathfrak{j}$ und wird mit $n(\mathfrak{j})$ bezeichnet.

Satz. *Ist $\mathfrak{a}$ ein Ideal des Körpers $k(\vartheta)$ und bilden:*

$$\begin{aligned} \alpha_1 &= a_{11}\omega_1 + a_{12}\omega_2 + a_{13}\omega_3 \\ \alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2 + a_{23}\omega_3 \\ \alpha_3 &= a_{31}\omega_1 + a_{32}\omega_2 + a_{33}\omega_3 \end{aligned}$$

eine Basis des Ideals $\mathfrak{a}$, so ist $n(\mathfrak{a}) = |(a_{11}a_{22}a_{33})|$.

Beweis An Stelle der beliebig gewählten Körperbasis nehme man zuerst einmal als Basiszahlen 1, ω^*, ω_1^* und drücke alle Zahlen des Ideals durch diese Basis aus. Verfährt man alsdann bei der Aufstellung einer Basis des Ideals genau so wie bei der Aufstellung der Körperbasis, so erkennt man, daß als Basiszahlen für das Ideal drei Zahlen α_1^*, α_2^*, α_3^* gewählt werden können von der folgenden Form:

$$\begin{aligned} \alpha_1^* &= a, \\ \alpha_2^* &= a_1 + a_2\omega^*, \\ \alpha_3^* &= a_3 + a_4\omega^* + a_5\omega_1^*, \end{aligned}$$

wo jetzt a die kleinste positive durch $\mathfrak{a}$ teilbare ganze rationale Zahl ist und wo a_2, a_5 ebenfalls als positive ganze Zahlen vorausgesetzt werden dürfen.

Dann erhält man lauter mod $(\mathfrak{a})$ inkongruente Zahlen, indem man in der linearen Form:

$$\beta = u + u_1\omega^* + u_2\omega_1^*$$

die Koeffizienten u die Zahlen 1 bis a, ferner u_1 die Zahlen 1 bis a_2 und u_2 die Zahlen 1 bis a_5 unabhängig voneinander durchlaufen läßt.

Es ist keine der so aufgestellten Zahlen in $\mathfrak{a}$ enthalten, keine kann irgend einer andern mod $(\mathfrak{a})$ kongruent sein, aber jede beliebige Zahl des Körpers muß einer derselben mod $(\mathfrak{a})$ kongruent sein; d. h. es ist damit ein spezielles vollständiges Restsystem[1]) aufgestellt. Die Anzahl der in diesem Restsystem enthaltenen Zahlen ist insgesamt $a \cdot a_2 \cdot a_5$.

Drückt man endlich die Basis des Körpers 1, ω^*, ω_1^* wieder durch ω_1, ω_2, ω_3 aus, indem man die Substitution macht:

$$\begin{aligned} 1 &= u_{11}\omega_1 + u_{12}\omega_2 + u_{13}\omega_3, \\ \omega^* &= u_{21}\omega_1 + u_{22}\omega_2 + u_{23}\omega_3 \text{ usw.} \end{aligned}$$

---

1) Das oben aufgestellte Restsystem entspricht dem vollständigen Restsystem der *„kleinsten Reste"* im Gebiet der rationalen Zahlen, wo die Zahlen 1, 2, ... a ein solches Restsystem nach a bilden. Man könnte natürlich auch den Begriff der „absolut kleinsten Reste", die zwischen $-\frac{1}{2}a$ und $+\frac{1}{2}a$ gelegen sind, auf die algebraischen Zahlen und Ideale übertragen.

mit der Determinante $(u_{11}, u_{22}, u_{33}) = \pm 1$, so wird:

$$\alpha_i^* = b_{i1}\omega_1 + b_{i2}\omega_2 + b_{i3}\omega_3 \quad (i = 1, 2, 3),$$

und es ist nach dem Multiplikationssatz für Determinanten:

$$\begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix} = \begin{vmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{vmatrix} \begin{vmatrix} a & 0 & 0 \\ a_1 & a_2 & 0 \\ a_3 & a_4 & a_5 \end{vmatrix} = \pm a \cdot a_2 \cdot a_5.$$

Wenn man schließlich die Basis $\alpha_1^*, \alpha_2^*, \alpha_3^*$ durch $\alpha_1, \alpha_2, \alpha_3$ nach den Formeln:

$$\alpha_i = v_{i1}\alpha_1^* + v_{i2}\alpha_2^* + v_{i3}\alpha_3^* \quad (\text{für } i = 1, 2, 3),$$

(mit der Substitutionsdeterminante $(v_{11}, v_{22}, v_{33}) = \pm 1$) ausdrückt, und jetzt wieder:

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + a_{i3}\omega_3$$

schreibt, so wird:

$$\begin{vmatrix} a_{11} & a_{12} & a_{12} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix} \cdot \begin{vmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{vmatrix} = \pm a a_2 a_5.$$

Somit ist für alle Fälle:

$$n(\mathfrak{a}) = |(a_{11} a_{22} a_{33})|,$$

wie der Satz behauptet. Die Zahl $n(\mathfrak{a}) = a a_2 a_3$ ist zugleich immer eine Zahl des Ideals.

Die Bedeutung, welche die Zahl $n(\mathfrak{a})$ für das Ideal $\mathfrak{a}$ hat, daß sie die Anzahl nach $\mathfrak{a}$ inkongruenter Zahl bezeichnet, kommt auch der ganzen rationalen Zahl $|n(\alpha)| = |\alpha\alpha'\alpha''|$ für eine ganze Zahl α des Körpers zu (vgl. S. 51).

Für die Rechnung mit Idealen ist hauptsächlich der folgende Multiplikationssatz wichtig:

Satz. *Die Norm eines Produktes zweier Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *ist gleich dem Produkt der Normen der beiden Ideale:* $n(\mathfrak{a}) \cdot n(\mathfrak{b})$.

Beweis. Es sei α eine ganze Zahl des Körpers, welche durch $\mathfrak{a}$ teilbar ist, so daß $\frac{(\alpha)}{\mathfrak{a}}$ prim ist zu $\mathfrak{b}$. Dann stellt die Form

$$\alpha\eta + \xi$$

lauter mod $(\mathfrak{a}\mathfrak{b})$ inkongruente ganze Zahlen des Körpers vor, wenn ξ alle Zahlen eines vollständigen Restsystems nach $\mathfrak{a}$ und η ebenso alle Zahlen eines Restsystems nach $\mathfrak{b}$ durchläuft. Das ganze System dieser Zahlen enthält $n(\mathfrak{a}) \cdot n(\mathfrak{b})$ Zahlen; keine zwei Zahlen des Systems

können einander mod $(\mathfrak{a}\mathfrak{b})$ kongruent sein, während jede beliebige ganze Zahl des Körpers *einer* Zahl dieses Systems nach dem Modul $\mathfrak{a}\mathfrak{b}$ kongruent ist.

Es bleibt daher, wie der Satz verlangt:

$$n(\mathfrak{a}\mathfrak{b}) = n(\mathfrak{a}) \cdot n(\mathfrak{b}).$$

Die Norm eines Ideals ist stets eine Zahl, welche dem Ideal selbst angehört, man kann daher zu einem Ideal $\mathfrak{a}$ ein anderes Ideal $\bar{\mathfrak{a}}$, welches man als ein zu $\mathfrak{a}$ reziprokes Ideal bezeichnen kann, so bestimmen, daß die Gleichung gilt:

$$(n(\mathfrak{a})) = \mathfrak{a} \cdot \bar{\mathfrak{a}}.$$

Für zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ ist dann $(n(\mathfrak{a}\mathfrak{b})) = \mathfrak{a} \cdot \bar{\mathfrak{a}} \cdot \mathfrak{b} \cdot \bar{\mathfrak{b}}$.

Der Satz über die Bestimmung der Norm eines Ideals soll nun noch speziell auf Primideale angewendet werden.

Wenn $\mathfrak{p}$ ein Primideal ist, das in der rationalen Primzahl p aufgeht, so hat man, wie durch eine spezielle Diskussion leicht einzusehen ist, für die Normalbasis des Primideals *vier* Möglichkeiten. Entweder es ist diese Basis des Primideals $\mathfrak{p}$ (nach den Bezeichnungen des Satzes auf der vorhergehenden Seite):

$$p,\ a_1 + 1\,\omega^*,\quad a_3 + a_4\omega^* + 1\,\omega_1^*,$$

oder

$$p,\ a_1 + p\,\omega^*,\quad a_3 + a_4\omega^* + 1\,\omega_1^*,$$

oder

$$p,\ a_1 + 1\,\omega^*,\quad a_3 + a_4\omega^* + p\,\omega_1^*,$$

oder schließlich

$$p,\ a_1 + p\,\omega^*,\quad a_3 + a_4\omega^* + p\,\omega_1^*.$$

Entsprechend diesen vier Möglichkeiten ist $n(\mathfrak{p}) = p^e$, wo $e = 1$ oder 2 oder 3 zu setzen ist. Die Zahl e heißt der *Grad des Primideals* $\mathfrak{p}$. Man unterscheidet also Primideale ersten, zweiten oder dritten Grades, und die Norm eines Primideals $\mathfrak{p}$ ist stets eine Potenz p^e der durch $\mathfrak{p}$ teilbaren rationalen Primzahl.

Nach dieser Einführung der Norm eines Ideals und der Berechnung ihres numerischen Wertes durch die Koeffizienten der Basis kann man nun wieder die Sätze aufstellen, welche zur Berechnung der Idealklassen eines Körpers erforderlich sind.

45. Sätze von Minkowski zur Aufstellung der Idealklassen.

Im Falle eines quadratischen Zahlkörpers diente zur Aufstellung der Idealklassen der Satz, daß jede der verschiedenen Klassen minde-

stens ein Ideal enthält, dessen Norm kleiner als (oder höchstens gleich) $|\sqrt{d}|$ ist, wobei d die Diskriminante des Körpers bezeichnet.

Um diesen selben Satz jetzt für den jetzigen allgemeineren Fall aufzustellen, beweise ich zunächst folgende Tatsache:

Hilfssatz. *Jedes beliebige Ideal* $\mathfrak{a}$ *des Körpers* $k(\vartheta)$ *enthält eine Zahl* α, *deren Norm der Ungleichung* $|n(\alpha)| \leqq n(\mathfrak{a})|\sqrt{d}|$ *genügt.*

Beweis. $k(\vartheta)$ bedeute einen reellen Körper und $\alpha_1, \alpha_2, \alpha_3$ die Basis des Ideals $\mathfrak{a}$, welche in der Gestalt:

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + a_{i3}\omega_3 \quad (i = 1, 2, 3)$$

dargestellt sei. Dann kann man nach dem Satz von Minkowski über lineare Formen drei ganze rationale von Null verschiedene Zahlen x, y, z so bestimmen, daß die absoluten numerischen Beträge der drei Formen:

$$\begin{aligned} f_1 &= \alpha_1 x + \alpha_2 y + \alpha_3 z \\ f_2 &= \alpha_1' x + \alpha_2' y + \alpha_3' z \\ f_3 &= \alpha_1'' x + \alpha_2'' y + \alpha_3'' z \end{aligned}$$

resp. $\leqq \varkappa_1, \leqq \varkappa_2, \leqq \varkappa_3$ werden. Wie früher bedeuten hierbei $\varkappa_1, \varkappa_2, \varkappa_3$ drei positive Größen, deren Produkt gleich dem absoluten Betrag der Koeffizientendeterminante der drei Formen f_1, f_2, f_3, also gleich $|(\alpha_1, \alpha_2', \alpha_3'')|$ ist. Nach Einsetzen der α in diese Determinante folgt dann:

$$\varkappa_1\varkappa_2\varkappa_3 = |(\alpha_1\alpha_2'\alpha_3'')| = |(a_{11}a_{22}a_{33})\sqrt{d}|.$$

Wenn nun $f_1 = \alpha$, somit $f_2 = \alpha', f_3 = \alpha''$ gesetzt wird, so ist α eine Zahl des Ideals $\mathfrak{a}$ mit der Eigenschaft:

$$|n(\alpha)| \leqq \varkappa_1\varkappa_2\varkappa_3,$$

oder

$$|n(\alpha)| \leqq |n(\mathfrak{a})\sqrt{d}|,$$

w. z. b. w.

Wenn dagegen $k(\vartheta)$ ein imaginärer Körper, $k(\vartheta')$ der zugehörige konjugiert imaginäre und $k(\vartheta'')$ der konjugiert reelle Körper ist, so setze man an Stelle von f_1, f_2 die Formen:

$$f_1 = \frac{1}{\sqrt{2}}\{(\alpha_1 + \alpha_1')x + (\alpha_2 + \alpha_2')y + (\alpha_3 + \alpha_3')z\},$$

$$f_2 = \frac{1}{\sqrt{-2}}\{(\alpha_1 - \alpha_1')x + (\alpha_2 - \alpha_2')y + (\alpha_3 - \alpha_3')z\}.$$

Gleichzeitig nehme man $\varkappa_1 = \varkappa_2$, dann erhält man wie vorhin den Beweis der Richtigkeit des Satzes auch für imaginäre Körper, indem ja [wegen $f_1^2 + f_2^2 = (f_1 + \sqrt{-1}f_2)(f_1 - \sqrt{-1}f_2)$]:

$$\frac{f_1^2 + f_2^2}{2} = |\alpha_1 x + \alpha_2 y + \alpha_3 y|^2 = |(\alpha_1 x + \alpha_2 y + \alpha_3 z)(\alpha_1' x + \alpha_2' y + \alpha_3' z)|$$

ist.

Hiermit ist nun leicht der Fundamentalsatz zu beweisen:

Satz. *Jede Idealklasse eines Körpers $k(\vartheta)$ enthält mindestens ein Ideal, dessen Norm kleiner ist als der absolute Betrag der Quadratwurzel aus der Diskriminante des Körpers.*

Beweis. Es möge $\mathfrak{a}$ irgend ein Ideal des Körpers $k(\vartheta)$ sein und $\bar{\mathfrak{a}}$ ein zweites Ideal, das mit $\mathfrak{a}$ multipliziert ein Hauptideal liefert:

$$(\alpha) = \mathfrak{a} \cdot \bar{\mathfrak{a}}.$$

Nun existiert in dem Ideal $\bar{\mathfrak{a}}$ eine Zahl $\bar{\alpha}$, für welche $n(\bar{\alpha}) < n(\bar{\mathfrak{a}}) |\sqrt{d}|$ ausfällt; als Zahl des Ideals $\bar{\mathfrak{a}}$ ist $\bar{\alpha}$ teilbar durch $\bar{\mathfrak{a}}$, und man kann daher eine Gleichung ansetzen:

$$(\bar{\alpha}) = \bar{\mathfrak{a}} \cdot \mathfrak{a}_1,$$

woraus

$$n(\bar{\mathfrak{a}}\mathfrak{a}_1) = n(\bar{\alpha}) \leq n(\bar{\mathfrak{a}}) |\sqrt{d}|$$

folgt; also ist:

$$n(\mathfrak{a}_1) \leq |\sqrt{d}|.$$

Da nun aus $(\alpha) = \mathfrak{a}\bar{\mathfrak{a}}$ und $(\bar{\alpha}) = \bar{\mathfrak{a}}\mathfrak{a}_1$ folgt, daß $\mathfrak{a} \sim \mathfrak{a}_1$ ist, so enthält die Idealklasse, welcher $\mathfrak{a}$ angehört, wenigstens ein Ideal $\mathfrak{a}_1$ mit der Eigenschaft $n(\mathfrak{a}_1) < |\sqrt{d}|$. Das gleiche gilt für jede Idealklasse.

Um die Klassenanzahl eines beliebigen Körpers $k(\vartheta)$ auf direktem Wege zu erhalten, braucht man also nur die positiven ganzen rationalen Zahlen, welche kleiner als oder höchstens gleich $|\sqrt{d}|$ sind, in Faktoren zu zerlegen und zu untersuchen, welche dieser Idealfaktoren einander äquivalent sind.

Hiernach ergibt sich als nächste Aufgabe die Zerlegung der rationalen Primzahlen in Primfaktoren.

46. Die Berechnung der Primideale im Körper $k(\vartheta)$.

Es liege ein ganz bestimmter Körper vor, gegeben durch eine ganze Zahl ϑ, welche als genau bezeichnete Wurzel der mit *Zahlen*koeffizienten versehenen irreduziblen Gleichung:

$$G(x) = x^3 + a_1 x^2 + a_2 x + a_3 = 0.$$

definiert ist.

Man soll die *Primideale* $\mathfrak{p}$, $\mathfrak{p}_1$ usw. aufstellen, durch welche eine gegebene *rationale* Primzahl p teilbar ist.

Da jedes Primideal des Körpers in einer rationalen Primzahl aufgeht, so erhält man alle Primideale, indem man die Zerlegung der rationalen Primzahlen ausführt, d. h. indem man zeigt, wie man die Primidealfaktoren derselben berechnet.

Wir setzen zuerst voraus, daß die Primzahl p nicht aufgehen soll in der Diskriminante der Zahl ϑ, d. h. es sei:

$$d(\vartheta) \not\equiv 0, \ (p).$$

Nachdem früher gezeigt worden ist, daß jedes Ideal dargestellt werden kann als größter gemeinsamer Teiler von zwei ganzen Zahlen des Körpers, darf man ein Primideal $\mathfrak{p}$ stets in der Form anschreiben: $\mathfrak{p} = (p, \alpha)$, wo α eine ganze Zahl des Körpers bedeuten soll. Unter der Voraussetzung ferner, daß p nicht in $d(\vartheta)$ aufgeht, kann man für α stets eine Zahl von der Form $a + b\vartheta + c\vartheta^2$ mit ganzen rationalen Koeffizienten a, b, c wählen, wie leicht einzusehen ist.

In Nr. 42, S. 261 hat sich die Basis des Körpers in der Form ergeben:

$$\omega = 1, \quad \omega_1 = \frac{-A + a_1 + \vartheta}{D}, \quad \omega_2 = \frac{A^2 - a_1 A + a_2 + A\vartheta + \vartheta^2}{D^2 D_1},$$

wo D und D_1 bestimmte Teiler von $d(\vartheta)$ sind. Man darf daher für jede ganze Zahl α schreiben:

$$\alpha = \frac{a + b\vartheta + c\vartheta^2}{D^2 D_1}.$$

Ist nun $\mathfrak{p}$ der größte gemeinsame Teiler von p und α, so ist es auch größter gemeinsamer Teiler von p und $D^2 D_1 \alpha$, da p weder in D noch in D_1 aufgeht und folglich auch $\mathfrak{p}$ prim ist zu $D^2 D_1$. Es bleiben dann noch die zwei Fälle zu unterscheiden, daß $D^2 D_1 \alpha$ vom ersten oder zweiten Grad in ϑ ist, d. h. es ist entweder:

$$\mathfrak{p} = (p, \ a + b\vartheta),$$

oder ev.:

$$\mathfrak{p} = (p, \ a + b\vartheta + c\vartheta^2)$$

zu setzen. Man braucht aber nur die *einfachsten* Möglichkeiten für diese beiden Fälle aufzustellen und anzugeben, wie a, b, c ev. zu bestimmen sind, wenn $\mathfrak{p}$ in der rationalen Primzahl p aufgeht.

Es sei erstens:

$$\mathfrak{p} = (p, \ a + b\vartheta), \tag{1}$$

und b prim zu p. Da nun das Ideal außerdem jede lineare Kombination von p und α mit ganzen rationalen Zahlen, d. h. die Zahlen:

$$x \cdot p\vartheta + y(a + b\vartheta)$$

enthält, so gehört demselben immer auch eine Zahl an von der Form:

$$-A+\vartheta,$$

(wo A eine ganze rationale Zahl bezeichnet), indem man x, y stets so bestimmen kann, daß:

$$px+by=1$$

wird. Dann ist auch:

$$\mathfrak{p}=(p,\ -A+\vartheta), \tag{2}$$

weil ja aus p und $-A+\vartheta$ durch lineare Kombination (mit lauter zu p primen Zahlen) wieder $a+b\vartheta$ ableitbar ist.

Es bleibt also jetzt nur noch A zu bestimmen. Zu diesem Zweck multipliziert man $-A+\vartheta$ mit der dem Körper ebenfalls angehörenden Zahl:

$$(-A+\vartheta')(-A+\vartheta'')$$

und erhält:

$$-A^3-a_1A^2-a_2A-a_3,$$

also eine rationale ganze Zahl, welche von Null verschieden ist und welche teilbar sein muß durch p. Somit ist A eine Lösung der Kongruenz:

$$x^3+a_1x^2+a_2x+a_3\equiv 0,\ (p). \tag{3}$$

Wenn diese Kongruenz nicht lösbar ist, so hat p sicher keinen Teiler $\mathfrak{p}$ von der Form der Gleichung (1).

Zweitens sei:

$$\mathfrak{p}=(p,\ a+b\vartheta+c\vartheta^2),$$

und c prim zu p; dann ergibt sich analog wie oben, daß unbeschadet der Allgemeinheit $c=1$ gesetzt werden darf, d. h. es ist auch:

$$\mathfrak{p}=(p,\ a+b\vartheta+\vartheta^2), \tag{4}$$

und $\mathfrak{p}$ enthält nur solche Zahlen von der Gestalt $a_1+b_1\vartheta$, deren Koeffizienten a_1, b_1 *beide* durch p teilbar sind; andernfalls würde $\mathfrak{p}$ auf die zuerst angenommene Form (1) zurückkommen.

Wir multiplizieren nun $a+b\vartheta+\vartheta^2$ mit einer ganzen Zahl $z+\vartheta$, in der z eine noch unbestimmte ganze rationale Zahl bedeutet, und berücksichtigen, daß wegen der Bedingung $\vartheta^3+a_1\vartheta^2+a_2\vartheta+a_3=0$ die Gleichung gilt:

$$\begin{aligned}\mathfrak{p}&=(p,a+b\vartheta+\vartheta^2,az+(a+bz)\vartheta+(b+z)\vartheta^2+\vartheta^3,a_3+a_2\vartheta+a_1\vartheta^2+\vartheta^3,\ldots)\\&=(p,\ a+b\vartheta+\vartheta^2,\ az-a_3+(a+bz-a_2)\vartheta+(b+z-a_1)\vartheta^2,\ \ldots).\end{aligned}$$

Bestimmt man jetzt z als ganze rationale Zahl entsprechend der Kongruenz:

$$b-a_1+z\equiv 0,\ (p),$$

so ist nach der Bemerkung über die Zahlen des Ideals von der Form $a_1 + b_1 \vartheta$ auch:

$$a + bz - a_2 \equiv 0, \ (p),$$
$$az - a_3 \equiv 0, \ (p),$$

oder es folgt:

$$(a + b\vartheta + \vartheta^2)(z + \vartheta) \equiv a_3 + a_2\vartheta + a_1\vartheta^2 + \vartheta^3, \ (p). \tag{5}$$

Man erhält folglich a, b und $a + b\vartheta + \vartheta^2$, wenn man $a_3 + a_2\vartheta + a_1\vartheta^2 + \vartheta^3$ nach dem Modul p in ein Produkt aus einem linearen und einem quadratischen Faktor zerlegen kann.

Die Aufsuchung der Primideale, die in einer Primzahl p aufgehen, führt somit immer auf die Untersuchung der Wurzeln der Kongruenz:

$$x^3 + a_1x^2 + a_2x + a_3 \equiv 0, \ (p). \tag{6}$$

Es mögen der Deutlichkeit wegen nochmals die Sätze hier angeführt werden, welche für die Lösungen (Wurzeln) einer solchen Kongruenz gelten:

1.) Ist A eine Lösung der Kongruenz (6), so gilt nach dem Modul p eine Zerlegung:

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A)f_1(x) \equiv 0, \ (p),$$

wo $f_1(x)$ eine ganze rationale Funktion zweiten Grades ist.

2.) Die Kongruenz (6) kann höchstens drei voneinander verschiedene Lösungen besitzen.

Weil nun die Zerlegung eines Ideals (p) in Primideale nur auf eine einzige Weise möglich ist, können wir hiernach endgültig folgende Sätze formulieren:

I. Hat die Kongruenz (6) überhaupt keine Lösung, so ist p im Körper $k(\vartheta)$ unzerlegbar, oder es ist (p) ein Primideal dritten Grades.

II. Hat die Kongruenz (6) die einzige Lösung $x = A$ und schreibt man:

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A)(x^2 + bx + a), \ (p), \tag{7}$$

so ist p durch die Primideale:

$$\mathfrak{p} = (p, \ -A + \vartheta), \quad \mathfrak{p}_1 = (p, \ a + b\vartheta + \vartheta^2) \tag{8}$$

teilbar; $\mathfrak{p}$, $\mathfrak{p}_1$ sind Primideale ersten und zweiten Grades, und es ist:

$$(p) = \mathfrak{p} \cdot \mathfrak{p}_1.$$

III. Hat die Kongruenz (6) drei Lösungen A_1, A_2, A_3, ist also:

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A_1)(x - A_2)(x - A_3), \ (p), \tag{9}$$

so ist p durch die drei Primideale ersten Grades

$$\mathfrak{p}_i = (p, \ -A_i + \vartheta) \quad (i = 1, 2, 3)$$

teilbar, und es ist daher:

$$(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3.$$

Lassen wir die Voraussetzung, daß die Primzahl p nicht in $d(\vartheta)$ aufgehen soll, fallen, und nehmen also im Gegenteil an, daß p ein Teiler von $d(\vartheta)$ ist, so sind die für p geltenden Zerlegungen viel schwieriger abzuleiten und zu beweisen.

Für unsere Zwecke genügt es, die entsprechenden Tatsachen historisch anzuführen, ich beschränke mich auf eine kleine einleitende Betrachtung. Wegen der Beweise möge der Leser die unten verzeichnete Literatur nachsehen.

Wenn $d(\vartheta) \equiv 0, (p)$ ist, so hat die Kongruenz:

$$x^3 + a_1 x^2 + a_2 x + a_3 \equiv 0, (p)$$

eine mehrfach zählende Lösung $x = A_1$; es ist entweder:

$$x^3 + a_1 x^2 + a_2 x + a_3 \equiv (x - A_1)^2 (x - A_2), (p)$$

oder

$$x^3 + a_1 x^2 + a_2 x + a_3 \equiv (x - A_1)^3, (p).$$

Wenn nämlich $G'(x) = 3x^2 + 2a_1 x + a_2$ die Ableitung der Funktion $G(x)$ bezeichnet, so ist die notwendige und hinreichende Bedingung für eine gemeinsame Lösung der beiden Kongruenzen:

$$G(x) \equiv 0, (p) \quad \text{und} \quad G'(x) \equiv 0, (p)$$

eben:

$$d(\vartheta) \equiv 0, (p),$$

wie man direkt durch Elimination von x aus den beiden ersten Kongruenzen zeigen kann.

Ist aber A die gemeinsame Lösung von

$$G(x) \equiv 0, \quad G'(x) \equiv 0, (p),$$

und schreibt man:

$$G(x) \equiv (x - A) f_1(x), (p),$$

so ist

$$G'(x) \equiv f_1(x) + (x - A) f_1'(x), (p).$$

Aus dieser Darstellung von $G'(x)$ folgt ohne weiteres, daß $G'(x)$ nach dem Modul p nur dann durch $x - A$ teilbar sein, d. h. mit $G(x) = 0$ eine Wurzel gemeinsam haben kann, wenn $f_1(x) \equiv (x - A) f_2(x), (p)$ ausfällt, oder wenn $G(x)$ mod (p) eine Doppelwurzel besitzt:

$$G(x) \equiv (x - A)^2 f_2(x), (p).$$

Falls $d(\vartheta) \equiv 0, (p)$ ist, so würde man danach vielleicht zunächst vermuten, daß p durch das Quadrat eines Primideals teilbar ist; das wäre nicht immer richtig, vielmehr gilt der folgende, von Dedekind zuerst aufgestellte, von ihm und von Hensel[1]) bewiesene Satz:

1) R. Dedekind: Über den Zusammenhang zwischen der Theorie der

Satz. *Alle und nur diejenigen rationalen Primzahlen, welche in der Diskriminante d des Körpers enthalten sind, sind durch das Quadrat eines Primideals teilbar.*

Wir haben den gleichen Satz für den quadratischen Zahlkörper leicht beweisen können und durften dieses Resultat vermuten. Dabei ist der Satz so zu verstehen, daß eine in d enthaltene Primzahl durch $\mathfrak{p}^2$ oder gar durch $\mathfrak{p}^3$ teilbar ist. Zum Beweise dieses Satzes und für die Zerlegung der in $d(\vartheta)$ überhaupt aufgehenden Primzahlen muß man die allgemeine Form des Ideals annehmen:

$$\mathfrak{p} = (p,\ a\omega + b\omega_1 + c\omega_2,\ \ldots).$$

Man setzt, unter u, u_1, u_2 veränderliche Zahlen verstanden:

$$\xi = u\omega + u_1\omega_1 + u_2\omega_2$$

und nennt diese in u, u_1, u_2 lineare Form die *Fundamentalform* des Körpers. Dieselbe genügt einer Gleichung dritten Grades:

$$F = (x - \xi)(x - \xi')(x - \xi'') = x^3 + U_1x^2 + U_2x + U_3 = 0,$$

welche die *Fundamentalgleichung* heißt.

Wenn man drei ganze rationale Funktionen $F_i(x, u, u_1, u_2)$ für $i = 1, 2, 3$ mit ganzzahligen Koeffizienten hat, so daß nach dem Modul p für beliebige x, u, u_1, u_2, die folgende Kongruenz besteht:

$$F_1 \equiv F_2 \cdot F_3,\ (p),$$

so heißt F_1 nach dem Modul p *zerlegbar*, oder durch F_2, F_3 *teilbar nach* p. Wenn ferner F_1 nur durch eine solche Funktion P teilbar ist, welche ihrerseits kongruent F_1 mod (p) ist, oder welche kongruent einer ganzen rationalen Zahl mod (p) ist, so heißt F_1 eine *Primfunktion* nach p. Nun gelten ganz allgemein die folgenden Sätze, die ich direkt nach Hilberts Zahlbericht hier anführe:

I. Wenn $\mathfrak{p}$ ein in p aufgehendes Primideal f^{ten} Grades bezeichnet, so gibt es stets nach p eine Primfunktion $P(x, u, u_1, u_2)$ vom Grade f in x, welche, wenn man an Stelle von x die Fundamentalform ξ

Ideale und der Theorie der höheren Kongruenzen. Abhandl. der math. Klasse der kgl. Gesellschaft der Wissensch. zu Göttingen. 23. Band, 1878. Von dem Dedekindschen Beweis gänzlich verschieden ist der von K. Hensel: Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Teiler ihrer Diskriminante. Crelles Journ., 113. Bd. 1894. Eine kurze Zusammenfassung des Beweises und Bemerkungen über die numerische Berechnung findet man bei D. Hilbert: Zahlber., Kap. IV, S. 195. Herr Hensel hat sodann das Problem dieser Nummer auf Grund einer ganz neuen umfassenden Methode vollständig erledigt. Vergl. Jahresber. d. d. Math.-Ver., Bd. 6, und Gött. Nachr. 1897; ferner Crelles Journal, Bd. 127, 128, 129.

setzt, folgende Eigenschaften besitzt: die Koeffizienten der Potenzen und Produkte von u, u_1, u_2 in der Funktion $P(\xi, u, u_1, u_2)$ sind sämtlich durch $\mathfrak{p}$, aber nicht sämtlich durch $\mathfrak{p}^2$ und auch nicht sämtlich durch ein von $\mathfrak{p}$ verschiedenes, in p aufgehendes Primideal teilbar.

II. Ist die Zerlegung der rationalen Primzahl p in Primideale in der Form $(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$ gegeben, so gestattet die linke Seite F der Fundamentalgleichung im Sinne der Kongruenz nach p die Darstellung

$$F \equiv P_1^{e_1} P_2^{e_2} P_3^{e_3}, \ (p),$$

wo P_1, P_2, P_3 verschiedene Primfunktionen nach p von x, u, u_1, u_2 bedeuten, und überdies ist, wenn:

$$F = P_1^{e_1} P_2^{e_2} P_3^{e_3} + p\Phi$$

gesetzt wird, Φ eine ganzzahlige Funktion von x, u, u_1, u_2, welche nach p durch keine der Primfunktionen P_1, P_2, P_3 teilbar ist.

Insbesondere enthält der Satz II alle notwendigen und hinreichenden Angaben für die Zerlegung einer Primzahl p. Z. B. enthält $\mathfrak{p}_1$ die Zahlen, die man nach der Vorschrift des Satzes I aus $P_1(x, u, u_1, u_2)$ erhält, wenn man statt x die Fundamentalform ξ einsetzt. Indessen braucht man den Satz in seiner ganzen Allgemeinheit *nur* dann anzuwenden, wenn die fragliche Zahl p in $\frac{d(\vartheta)}{d}$ enthalten ist. Etwas weiter, als oben bewiesen wurde, gilt nämlich die folgende Behauptung:

Satz. *Ist die Zahl ϑ durch die Gleichung definiert:*

$$G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0,$$

und ist p eine rationale Primzahl, welche der Bedingung genügt $\frac{d(\vartheta)}{d} \not\equiv 0, \ (p)$, so liefert jede Zerlegung der Funktion $G(x)$ nach dem Modul p:

$$G(x) \equiv G_1(x)^{e_1} G_2(x)^{e_2} G_3(x)^{e_3}, \ (p)$$

eine Zerlegung der Zahl p in Primideale des Körpers $k(\vartheta)$ von der Gestalt:

$$(p) = (p, G_1(\vartheta))^{e_1}(p, G_2(\vartheta))^{e_2}(p, G_3(\vartheta))^{e_3}.$$

Ein ziemlich umfangreiches Zahlenmaterial zu den gesamten Entwicklungen dieses vierten Abschnitts findet sich in der bereits zitierten Göttinger Dissertation von L. W. Reid, aus welcher ich einige Beispiele hier anführe.

1. Beispiel. Es sei ϑ eine Wurzel der Gleichung:

$$x^3 + x + 1 = 0,$$

dann ist $d(\vartheta) = -31$ und ebenso $d = -31$. Als Basis kann daher

$1, \vartheta, \vartheta^2$ gewählt werden. Um die Klassenanzahl des Körpers $k(\vartheta)$ zu bestimmen, hat man die Zerlegung der Zahlen 2, 3, 5 auszuführen. Da diese Zahlen prim sind zu d, so sind hierzu wieder nur die Zerlegungen der Kongruenz

$$x^3 + x + 1 \equiv 0,$$

nach den Moduln 2, 3, 5 notwendig. Man findet, daß 2 und 5 unzerlegbar sind, während

$$3 = (-\vartheta + 1)(\vartheta^2 + \vartheta + 2)$$

wird. Es ist somit $h = 1$. Als Einheiten finden sich ferner:

$$\vartheta, \quad \vartheta + 1.$$

2. Beispiel. ϑ sei eine Wurzel der Gleichung:

$$x^3 + 6x + 8 = 0,$$

dann ist $d(\vartheta) = -2592 = -2^5 \cdot 3^4$. Als Basis kann man nehmen: $1, \vartheta, \frac{\vartheta^2}{2}$, und daraus folgt für d der Wert $d = -2^3 \cdot 3^4$. Nun wird:

$$(2) = \left(2, 1 + \vartheta + \frac{\vartheta^2}{2}\right)^2 \left(2, \frac{\vartheta^2}{2}\right),$$

$$(3) = (3, \vartheta - 1)^3,$$

$$(5) = (5, \vartheta - 1)(5, 2 + \vartheta + \vartheta^2),$$

$$(7) = (7, \vartheta - 2)(7, 3 + 2\vartheta + \vartheta^2).$$

Diese Ideale verteilen sich auf *drei* Klassen. Schließlich findet sich als Einheit: $\vartheta + 1$.

3. Beispiel. Endlich möge ϑ eine Wurzel der Gleichung:

$$x^3 - 8x + 4 = 0$$

sein, dann ist $d(\vartheta) = +1616 = 2^4 \cdot 101$. In diesem Fall kann als Basis z. B. genommen werden: $1, \vartheta, \frac{\vartheta^2}{2}$, wonach $d = 2^2 \cdot 101$ wird. Es ergibt sich:

$$2 = \left(\frac{\vartheta^2}{2}\right)^3 (132\vartheta^2 + 68\vartheta - 1023),$$

$$3 = (\vartheta - 1)(\vartheta^2 + \vartheta - 7).$$

Die Klassenanzahl ist $h = 1$, und Einheiten sind u. a.:

$$2\vartheta - 1, \quad 132\vartheta^2 + 68\vartheta - 1023.$$

47. Die Einheiten des Körpers $k(\vartheta)$.

Unter allen ganzen Zahlen des Körpers $k(\vartheta)$ sind diejenigen von besonderer Bedeutung, deren Norm gleich ± 1 ist, und die man wieder als **Einheiten** des Körpers bezeichnet.

Ist ε eine solche ganze Zahl, also

$$\varepsilon\varepsilon'\varepsilon'' = \pm 1,$$

so folgt zunächst, daß auch $\frac{1}{\varepsilon}$ eine ganze Zahl des Körpers ist. Denn es ist

$$\varepsilon'\varepsilon'' = \frac{\pm 1}{\varepsilon},$$

und $\varepsilon'\varepsilon''$ ist eine ganze Zahl des Körpers $k(\vartheta)$. Offenbar sind ± 1 selbst die einfachsten Einheiten des Körpers. Wenn ferner ε eine von ± 1 verschiedene Einheit des Körpers bezeichnet, so stellt auch jede Potenz $\pm \varepsilon^e$ mit ganzzahligem positivem oder negativem Exponenten e eine Einheit dar, weil offenbar auch $\varepsilon^e\varepsilon'^e\varepsilon''^e = (\varepsilon\varepsilon'\varepsilon'')^e = \pm 1$ ist.

Falls der Körper $k(\vartheta)$ nebst seinen Konjugierten *reell* ist, kann eine Einheit ε nicht irgendwelche zweite oder dritte Wurzel aus der Zahl ± 1 sein, insofern diese Einheitswurzeln komplexe Zahlen sind. Aber auch falls $k(\vartheta)$ reell ist und $k(\vartheta')$ und $k(\vartheta'')$ imaginäre Körper sind, so kann in keinem der drei Körper eine andere Einheitswurzel als ± 1 vorkommen. Angenommen nämlich, z. B.

$$\eta' = \frac{a\vartheta'^2 + b\vartheta' + c}{N}$$

wäre eine komplexe Einheitswurzel aus $k(\vartheta')$, so wären die Konjugierten η'' und η auch Einheitswurzeln; dann müßte aber $\eta = \pm 1$ sein, und es müßte folglich für ϑ eine Gleichung (mit rationalen Koeffizienten a, b, c, N):

$$a\vartheta^2 + b\vartheta + c = \pm N$$

bestehen. Weil indessen für ϑ die Definitionsgleichung gilt:

$$\vartheta^3 + a_1\vartheta^2 + a_2\vartheta + a_3 = 0,$$

so ließe sich bekanntlich ϑ aus den beiden Gleichungen als rationale Zahl berechnen, entgegen den Voraussetzungen über ϑ. Es muß $a = 0$, $b = 0$ und $c = \pm N$, und somit auch $\eta' = \pm 1$ sein.

Auf die gleiche Weise folgt, daß jede Einheit ε des Körpers, für welche $|\varepsilon| = 1$ ist, selbst gleich ± 1 sein muß. Denn wenn ε reell ist, dann folgt aus $|\varepsilon| = 1$ eben $\varepsilon = \pm 1$, und wenn ε komplex ist, so folgt aus $|\varepsilon| = 1$ auch $|\varepsilon'| = |\varepsilon| = 1$, $|\varepsilon''| = 1$, wonach die reelle Einheit $\varepsilon'' = \pm 1$ sein muß, und folglich ε, ε' ebenfalls.

Nach dieser Einleitung beweisen wir nun folgenden Hilfssatz:

Satz.[1]) *In jedem (reellen oder imaginären) Zahlkörper $k(\vartheta)$ vom dritten Grad existiert eine von ± 1 verschiedene Einheit.*

Der Beweis dieses Satzes unterscheidet sich nicht prinzipiell von dem Beweis desselben Satzes für reelle quadratische Körper, so daß ich mich hier kurz fassen kann.

Beweis. I. Es sei zuerst die Diskriminante d des Körpers positiv, also alle drei Körper $k(\vartheta)$, $k(\vartheta')$, $k(\vartheta'')$ reell. A, A_1, A_2 seien drei beliebige reelle positive Zahlen, deren Produkt

$$A \cdot A_1 \cdot A_2 = |\sqrt{d}| \tag{1}$$

ist.

Dann zeigt man auf Grund des Minkowskischen Satzes über lineare Formen in derselben Weise, wie dies schon früher geschah, daß man stets eine *ganze* Zahl α in $k(\vartheta)$ bestimmen kann, für welche:

$$|\alpha| \leq A, \quad |\alpha'| \leq A_1, \quad |\alpha''| \leq A_2, \tag{2}$$

ausfällt.

Weil aber α eine *ganze* Zahl des Körpers ist, so muß notwendig

$$|\alpha \cdot \alpha' \cdot \alpha''| \geqq 1$$

sein, und hieraus folgt

$$|\alpha| \geqq \frac{1}{|\alpha' \alpha''|},$$

oder unter Berücksichtigung der Gleichungen (2) und (1) ferner:

$$|\alpha| \geqq \frac{1}{A_1 A_2} \quad \text{resp.} \quad |\alpha| \geqq \frac{A}{|\sqrt{d}|}.$$

Man hat somit für α und seine Konjugierten die Ungleichungen:

$$\left.\begin{aligned} A &\geqq |\alpha| \geqq \frac{A}{|\sqrt{d}|} \\ A_1 &\geqq |\alpha'| \geqq \frac{A_1}{|\sqrt{d}|} \\ A_2 &\geqq |\alpha''| \geqq \frac{A_2}{|\sqrt{d}|} \end{aligned}\right\}. \tag{3}$$

Die letzte Gleichung könnte auch geschrieben werden:

$$\frac{\sqrt{d}}{A \cdot A_1} \geqq |\alpha''| \geqq \frac{1}{A \cdot A_1}.$$

---

1) P. G. Lejeune Dirichlet, Werke, Bd. 1, S. 642. Teile des allgemeinsten Satzes ibid. S. 622 und für kub. Zahlen S. 632. H. Minkowski, Geom. d. Zahlen Nr. 44, S. 137 ff. D. Hilbert, Bericht, Kap. VI, sp. § 19 u. 20, S. 214 ff.

Nun nehme man drei neue reelle positive Zahlen an:

$$B = \frac{A}{|\sqrt{d}|}, \quad B_1 = \frac{A_1}{|\sqrt{d}|}, \quad B_2 = \frac{A_2 |\sqrt{d}|^3}{|\sqrt{d}|},$$

deren Produkt wieder

$$B B_1 B_2 = |\sqrt{d}|$$

ist. Dann existiert eine ganze Zahl β in $k(\vartheta)$, welche den folgenden Ungleichungen genügt:

$$\left.\begin{array}{l} B \geqq |\beta| \geqq \dfrac{B}{|\sqrt{d}|} \\ B_1 \geqq |\beta'| \geqq \dfrac{B_1}{|\sqrt{d}|} \\ B_2 \geqq |\beta''| \geqq \dfrac{B_2}{|\sqrt{d}|} \end{array}\right\}, \tag{4}$$

wo an Stelle der letzten Ungleichung auch geschrieben werden kann:

$$\frac{|\sqrt{d}|}{B B_1} \geqq |\beta''| \geqq \frac{1}{B B_1}.$$

Jetzt setze man wieder

$$C = \frac{B}{|\sqrt{d}|}, \quad C_1 = \frac{B_1}{|\sqrt{d}|}, \quad C_2 = \frac{B_2 |\sqrt{d^3}|}{|\sqrt{d}|}$$

und bestimme in analoger Weise, wie eben α und β bestimmt wurden, ein ganze Zahl γ.

Setzt man dieses Verfahren unbeschränkt fort, so erhält man eine nicht abbrechende Reihe von ganzen algebraischen Zahlen, welche Ungleichungen von der Form (3) und (4) genügen.

Für die Zahlen des Körpers $k(\vartheta)$ und auch $k(\vartheta')$ lassen sich diese Ungleichungen zusammenfassen in der folgenden Form:

$$A \geqq |\alpha| \geqq \frac{A}{|\sqrt{d}|} \geqq |\beta| \geqq \frac{A}{|\sqrt{d^2}|} \geqq |\gamma| \geqq \frac{A}{|\sqrt{d^3}|} \geqq \delta \geqq \frac{A}{|\sqrt{d^4}|} \geqq \cdots$$

Weil die Diskriminante $|d| > 1$ ist, so bilden also die Zahlen $|\alpha|$, $|\beta|$, ..., ebenso $|\alpha'|$, $|\beta'|$, ... eine Reihe *abnehmender* Zahlen, während man für α'' usw. durch Zusammenziehung der Ungleichungen (3) und (4) usw. folgert, daß $|\alpha''|$, $|\beta''|$, ... eine Reihe *zunehmender* Zahlen bildet.

Benützt man jetzt den Umstand, daß die Hauptideale (α), (β), (γ), ... eine nicht abbrechende Reihe von Idealen sind mit Normen $\leqq |\sqrt{d}|$ und berücksichtigt, daß es überhaupt nur eine endliche Anzahl von Idealen geben kann, deren Normen kleiner sind als eine

endliche Zahl, so müssen in der Reihe (α), (β), (γ) usw. unendlich vielmal zwei Ideale einander gleich sein.

Ist etwa $(\alpha) = (\gamma)$ und $|\alpha| > |\gamma|$, so stellt nun der Quotient $\varepsilon = \frac{\alpha}{\gamma}$ eine von ± 1 verschiedene *Einheit* des Körpers dar.

Wegen der Ungleichungen für α, γ usw. ist

$$|\varepsilon| > 1, \quad |\varepsilon'| > 1 \quad \text{und} \quad |\varepsilon''| < 1,$$

wenn

$$\varepsilon' = \frac{\alpha'}{\gamma'} \quad \text{und} \quad \varepsilon'' = \frac{\alpha''}{\gamma''}$$

gesetzt ist. Durch direkte Betrachtung sieht man ferner, daß $|\varepsilon|$ und $|\varepsilon'|$ nicht gleich sein können.

Es ist leicht einzusehen, daß auf analoge Weise eine Einheit η abgeleitet werden kann, für welche $|\eta| > 1$, $|\eta'| < 1$, $|\eta''| > 1$ ausfällt.

II. Es sei zweitens die Diskriminante d negativ. Wir nehmen an, daß $k(\vartheta)$ reell ist, während $k(\vartheta')$, $k(\vartheta'')$ die imaginären Körper sind, und wählen zwei positive reelle Zahlen A, A_1, so daß $A \cdot A_1^2 = |\sqrt{d}|$ ist, dann läßt sich eine ganze Zahl α so bestimmen, daß

$$|\alpha| \leqq A, \quad |\alpha'| \leqq A_1 \tag{2a}$$

ist, wozu noch wegen $|\alpha'| = |\alpha''|$ die Ungleichung $|\alpha''| \leqq A_1$ kommt.

Wie oben ergibt sich dann:

$$\left.\begin{aligned} A &\geqq |\alpha| \geqq \frac{A}{|\sqrt{d}|} \\ A_1 &\geqq |\alpha'| \geqq \frac{A_1}{|\sqrt{d}|} \end{aligned}\right\}. \tag{3a}$$

Nun setze man weiter:

$$B = \frac{A}{|\sqrt{d}|}, \quad B_1 = A_1 |\sqrt{d}|,$$

so daß:

$$BB_1^2 = |\sqrt{d}|,$$

wird und konstruiere die ganze Zahl β in $k(\vartheta)$, so daß

$$|\beta| \leqq B, \quad |\beta'| = |\beta''| \leqq B_1.$$

Durch Wiederholung dieses Verfahrens erhält man wieder unendlich viele Ideale (α), (β), ..., aus denen man wieder wie im Fall $d > 0$ auf die Existenz einer von ± 1 verschiedenen Einheit ε in $k(\vartheta)$ und ε', ε'' in $k(\vartheta')$ resp. $k(\vartheta'')$ schließt.

Bei der Ableitung ergibt sich übrigens noch, im Gegensatz zu vorhin:

$$|\varepsilon| > 1 \quad \text{und gleichzeitig} \quad |\varepsilon'| = |\varepsilon''| < 1,$$

oder

$$|\eta| < 1, \text{ wenn gleichzeitig } |\eta'| = |\eta''| > 1 \text{ ist.}$$

Damit ist der Hilfssatz bewiesen, und wir können nun zu dem Beweise des Dirichletschen Fundamentalsatzes übergehen, für dessen Fassung ich die folgende auf beliebige Körper leicht übertragbare allgemeinere Form wähle:

Satz. *Befinden sich unter den drei konjugierten Körpern* $k(\vartheta)$, $k(\vartheta')$ *und* $k(\vartheta'')$ *reelle Körper in der Anzahl* r_1, *und* $r_2 = \frac{3 - r_1}{2}$ *Paare konjugiert imaginäre Körper, so gibt es in jedem der drei Körper (z. B. in* $k(\vartheta)$*)* $r = r_1 + r_2 - 1$ *Grundeinheiten* $\varepsilon_1, \ldots \varepsilon_r$ *von der Beschaffenheit, daß jede beliebige andere Einheit* ξ *des Körpers sich auf eine einzige Weise in der Form darstellen läßt:*

$$\xi = \pm\, \varepsilon_1^{e_1}, \ldots \varepsilon_r^{e_r},$$

wo $e_1, \ldots e_r$ *positive oder negative ganze rationale Zahlen bedeuten.*

Man hat offenbar zwei Möglichkeiten. Wenn $r_1 = 1$ und $r_2 = 1$ ist, so existiert in jedem der drei Körper dritten Grades *eine* Grundeinheit; wenn dagegen $r_1 = 3$, $r_2 = 0$ ist, so existieren je *zwei* Grundeinheiten.

Der Beweis des letzteren Falles ist der schwierigere, derselbe ist von Minkowski und sodann von Hilbert sehr durchsichtig ausgeführt. Ich will hier den von Herrn Minkowski entwickelten Beweis wiedergeben.

Beweis. Es seien also $k(\vartheta)$ und $k(\vartheta')$, $k(\vartheta'')$ drei reelle Körper. Dann gibt es zwei Einheiten ε, η, von denen wir nach unserem Hilfssatz voraussetzen dürfen, daß:

$$|\varepsilon| > 1, \quad |\varepsilon'| > 1, \quad |\varepsilon''| < 1$$
$$|\eta| > 1, \quad |\eta'| < 1, \quad |\eta''| > 1,$$

ist.

Wenn nun ξ irgend eine beliebige ganze Zahl des Körpers bezeichnet, so heißen die reellen Werte $\log|\xi|$, $\log|\xi'|$ und $\log|\xi''|$ die Logarithmen der Zahl ξ, und es möge zur Abkürzung geschrieben werden:

$$l(\xi) = \log|\xi|, \quad l_1(\xi) = \log|\xi'|, \quad l_2(\xi) = \log|\xi''|.$$

Wegen $\xi\xi'\xi'' = \pm 1$ erfüllen dann die Logarithmen einer *Einheit* ξ stets die Gleichung

$$f = l(\xi) + l_1(\xi) + l_2(\xi) = 0, \tag{1}$$

und andererseits muß *jede Einheit* des Körpers zu einer Lösung der Gleichung $f=0$ führen.

Falls einer oder alle drei Logarithmen $l(\xi)$, $l_1(\xi)$ oder $l_2(\xi)$ gleich Null werden, so muß nach der in der Einleitung angestellten Betrachtung notwendig $\xi = \pm 1$ sein. Um also alle Einheiten des Körpers zu erhalten, hat man alle Lösungen der Gleichung (1): $f=0$ aufzusuchen, deren Werte sämtlich von Null verschieden sind.

Man setze nun

$$f_2(\xi) = h\,l(\xi) + h_1 l_1(\xi), \tag{2}$$

und bestimme h, h_1 so, daß

$$f_2(\eta) = h\,l(\eta) + h_1 l_1(\eta) > 0$$

wird. Indem man etwa $h_1 = -l(\varepsilon)$ und $h = l_1(\varepsilon)$ setzt, wird von selbst:

$$f_2(\eta) = l_1(\varepsilon)l(\eta) - l(\varepsilon)l_1(\eta) > 0,$$

weil $l_1(\eta)$ wegen $|\eta'| < 1$ negativ ist, während $l(\varepsilon)$, $l_1(\varepsilon)$, $l(\eta)$ positive, von Null verschiedene Zahlen sind.

Daher kann jede Lösung der Gleichung (1) in der Gestalt angenommen werden:

$$\left.\begin{aligned} l(\xi) &= s_1 l(\varepsilon) + s_2 l(\eta) \\ l_1(\xi) &= s_1 l_1(\varepsilon) + s_2 l_1(\eta) \\ l_2(\xi) &= s_1 l_2(\varepsilon) + s_2 l_2(\eta) \end{aligned}\right\}, \tag{3}$$

wo s_1 und s_2 beliebige reelle Zahlenwerte sind.

In der Tat befriedigen die drei Werte der Gleichungen (3) die Gleichung (1) identisch, und es lassen sich zu einer gegebenen Lösung $l(\xi)$, $l_1(\xi)$, $l_2(\xi)$ aus den beiden ersten Gleichungen die Zahlen s_1, s_2 wegen der Bedingung $f_2(\eta) > 0$ als endliche Zahlen und nur auf eine einzige Weise berechnen, weil die Gleichungen (3) alsdann widerspruchsfrei sind.

Für $\xi = \varepsilon$ erhält man aus (3) $s_1 = 1$ und $s_2 = 0$, ferner wird für $\xi = \eta$: $s_1 = 0$, $s_2 = 1$. Es soll nun zunächst gezeigt werden, daß nur für eine *endliche* Anzahl Einheiten gleichzeitig

$$0 \leqq s_1 < 1, \quad 0 \leqq s_2 < 1 \tag{4}$$

sein kann.

Wenn nämlich für eine Einheit ξ diese Ungleichungen erfüllt sind, so ist

$$|l(\xi)| < |l(\varepsilon)| + |l(\eta)|,$$

$$|l_i(\xi)| < |l_i(\varepsilon)| + |l_i(\eta)| \quad (\text{für } i = 1, 2),$$

d. h. die absoluten Beträge $|\xi|$, $|\xi'|$, $|\xi''|$ sind kleiner als drei bestimmte nur von ε und η abhängige endliche Zahlen. Stellt nun

$$\xi = x + y\omega_1 + z\omega_2$$

eine ganze Zahl des Körpers vor, und berechnet man umgekehrt x, y, z aus den drei Gleichungen

$$\begin{aligned} x + \omega_1 y + \omega_2 z &= \xi, \\ x + \omega_1' y + \omega_2' z &= \xi', \\ x + \omega_1'' y + \omega_2'' z &= \xi'', \end{aligned}$$

so erhält man $x = \lambda_1 \xi + \lambda_2 \xi' + \lambda_3 \xi''$ und ähnliche Werte für y und z. Nun sind λ_1, λ_2, λ_3 konstante Werte mit endlichen absoluten Beträgen, und wenn die absoluten Beträge der $|\xi|$ unterhalb endlicher Grenzen liegen, so ist auch $|x|$ unterhalb einer endlichen Zahl gelegen, ebenso $|y|$, $|z|$. Daraus folgt aber, daß für x, y, z von vornherein nur eine endliche Anzahl von Kombinationen ganzer rationaler Zahlen gewählt werden können, so daß jedesmal $|\xi|$, $|\xi'|$, $|\xi''|$ unter einer endlichen Zahl bleiben.

Die sämtlichen Einheiten ξ, deren Darstellungen in der Form (3) so beschaffen sind, daß

$$0 \leq s_1 < 1, \quad 0 \leq s_2 < 1$$

wird, kann man jetzt in zwei Klassen ordnen.

Die erste Klasse enthalte die Einheiten, für welche $s_2 = 0$ ist, die zweite Klasse diejenigen, für welche $s_2 > 0$ ist. Alsdann bestimmt man in der ersten Klasse diejenige Einheit ε_1, für welche s_1 *seinen kleinsten von Null verschiedenen Wert* S_1 annimmt, und in der zweiten Klasse ebenso eine Einheit ε_2, für welche s_2 *seinen kleinsten Wert* S_2 annimmt.

Dann gibt es keine Einheit außer ± 1, für deren Darstellung in der Form (3) gleichzeitig die Bedingungen gelten würden:

$$0 \leq s_1 < S_1 \quad \text{und} \quad 0 < s_2 < S_2. \tag{5}$$

Bezeichnet nun ξ eine beliebige Einheit des Körpers und e_1, e_2 zwei zunächst noch unbekannte ganze rationale positive oder negative Zahlen, dann ist auch $\dfrac{\xi}{\varepsilon_1^{e_1}\varepsilon_2^{e_2}}$ eine Einheit des Körpers, deren Logarithmen L_2 und:

$$\begin{aligned} L &= l(\xi) - e_1 l(\varepsilon_1) - e_2 l(\varepsilon_2), \\ L_1 &= l_1(\xi) - e_1 l_1(\varepsilon_1) - e_2 l_1(\varepsilon_2) \quad \text{sind.} \end{aligned}$$

Schreibt man $l(\varepsilon_1) = S_1 l(\varepsilon)$ und $l(\varepsilon_2) = S l(\varepsilon) + S_2 l(\eta)$ und sucht für L, L_1 die Darstellung analog den Gleichungen (3), so erhält man:

$$s_1 = \frac{l_1(\xi)\, l(\eta) - l(\xi)\, l_1(\eta)}{f_2(\eta)} - e_1 S_1 - e_2 S,$$

$$s_2 = \frac{-\, l_1(\xi)\, l(\varepsilon) + l(\xi)\, l_1(\varepsilon)}{f_2(\eta)} - e_2 S_2.$$

Da $f_2(\eta) > 0$ ist, so kann man aus der zweiten Gleichung zunächst e_2, sodann aus der ersten e_1 als ganze positive oder negative rationale Zahlen so bestimmen, daß s_1 resp. s_2 den Ungleichungen (5) genügen. Alsdann muß aber direkt:

$$L = 0, \quad L_1 = 0$$

und folglich $L_2 = 0$ sein, oder es wird

$$\frac{\xi}{\varepsilon_1^{e_1} \varepsilon_2^{e_2}} = \pm 1, \quad \text{resp.} \quad \xi = \pm\, \varepsilon_1^{e_1} \varepsilon_2^{e_2},$$

und damit ist der Dirichletsche Satz bewiesen, wenn $d > 0$ ist, also wenn alle drei konjugierten Körper reell sind.

Den zweiten Fall, in dem $d < 0$ ist, und $k(\vartheta)$ einen reellen Körper, $k(\vartheta')$, $k(\vartheta'')$ ein Paar konjugiert imaginäre Körper bezeichnen, brauchen wir überhaupt nicht ausführlich zu behandeln.

Ist nämlich ε_1 diejenige Einheit in $k(\vartheta)$, welche unter allen Einheiten in $k(\vartheta)$, deren absoluter Wert > 1 ist, den *kleinsten* Betrag hat, so zeigt man ganz ähnlich, wie dies für die Einheiten des reellen quadratischen Körpers geschah, daß eine beliebige Einheit ξ des Körpers in der Form darstellbar ist:

$$\xi = \pm\, \varepsilon_1^{e_1},$$

wo e_1 eine ganze rationale, positive oder negative Zahl bedeutet.

Der Dirichletsche Satz ist damit für die Körper dritten Grades vollständig bewiesen.

Fünfter Abschnitt.

Relativkörper.

Die Lehre von den quadratischen und kubischen Zahlkörpern, welche in den vorhergehenden Abschnitten behandelt wurde, bildet nur den Anfang einer ganz allgemeinen Theorie der Zahlkörper. Gegenstand derselben ist die Untersuchung der Eigenschaften von solchen ganzen algebraischen Zahlen, welche irreduziblen Gleichungen von einem beliebigen Grad n genügen.

Auf diese Theorie soll hier nicht weiter eingegangen werden. Wir wollen aber noch eine andere Verallgemeinerung der Begriffe der Zahlentheorie in ihren Grundzügen auseinandersetzen, weil sich hier noch ein Feld für viele weitere fruchtbringende Arbeit darbietet, und weil gerade diese neuen Begriffe wichtige Anwendungen in der Lösung schwieriger fundamentaler Aufgaben der Algebra und der Funktionentheorie gefunden haben. Ihre Einführung schließt sich sehr natürlich an die Aufstellung und den Beweis der allgemeinen Reziprozitätsgesetze in Zahlkörpern an.

In Nr. 24 und 25 wurde für das quadratische Reziprozitätsgesetz für rationale Primzahlen, d. h. für die Formel:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

nebst den Ergänzungssätzen, ein Beweis geführt, welcher darauf beruhte, daß über dem Bereich der rationalen Zahlen ein Zahlkörper $k(\sqrt{p})$ resp. $k(\sqrt{\pm q})$ aufgebaut wurde, dessen Eigenschaften dann das Reziprozitätsgesetz lieferten. Da wir nun die Lehre von den Kongruenzen ohne weiteres auf die Zahlen und Ideale eines Zahlkörpers übertragen konnten, so drängt sich die Frage auf, ob auch die Reziprozitätsgesetze, welche für die Lösungen einander zugeordneter Zahlenkongruenzen bestehen, auf die Zahlen und Ideale eines Zahlkörpers erweitert werden können. Liegt ein quadratischer Zahlkörper vor und be-

schränkt man sich auf die Betrachtung quadratischer Kongruenzen, also auf eine Ausdehnung des quadratischen Reziprozitätsgesetzes[1]), so ergibt sich ganz von selber ein Prüfstein für die Allgemeinheit der bisher entwickelten Gesichtspunkte. Man wird nämlich in konsequenter Fortbildung der Beweismethode für die Formel:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

versuchen, über dem gegebenen quadratischen Zahlkörper einen neuen quadratischen Körper, den *„relativ quadratischen Körper"* aufzubauen, um dann aus den Eigenschaften dieses „Relativkörpers" das gesuchte Gesetz abzuleiten. In der Tat führt dieser Versuch zum Ziel. Es hat Herr Hilbert[2]) auf diesem Wege das quadratische Reziprozitätsgesetz für eine umfassende Klasse von Grundkörpern bewiesen.[3]) Um die Richtung zu charakterisieren, in welcher sich seine schwierigen und tiefgehenden Untersuchungen bewegen, will ich mich noch mit dem einfachsten Fall des quadratischen Relativkörpers in bezug auf einen quadratischen Grundkörper beschäftigen und die neuen Begriffe hauptsächlich durch Zahlenbeispiele erläutern.

48. Grundbegriffe und Definitionen.

Es sei ein quadratischer Zahlkörper $k(\sqrt{m})$ gegeben mit der ganzen rationalen quadratfreien Grundzahl m. μ sei irgend eine von m, 0 und 1 verschiedene ganze Zahl dieses Körpers, welche nur nicht das Quadrat einer ganzen Zahl des Körpers ist, ferner bezeichnen α,

1) Den einfachsten Fall des quadratischen Reziprozitätsgesetzes für die Zahlen des Körpers $k(\sqrt{-1})$ hat schon C. F. Gauß behandelt. Werke, Bd. II, S. 130, Theoria resid. biquadr. Comm. II, Nr. 60 (56—60) und Anzeige dieser Abhandlung, Werke, Bd. II, S. 172.

2) Hilbert, Über die Theorie des relativquadratischen Zahlkörpers. Math. Annalen, Bd. 51, S. 1—127.

Einen speziellen Fall dieser Theorie untersucht H. Dörrie in seiner Dissertation „Das quadratische Reziprozitätsgesetz im quadratischen Zahlkörper mit der Klassenanzahl 1". Göttingen 1898. Als Zahlenbeispiel ist in dieser Diss. die Behandlung des Körpers $k(\sqrt{-3})$ durchgeführt.

3) Mit dem weiteren Ausbau der Hilbertschen Theorie beschäftigte sich u. a. sehr eingehend Ph. Furtwängler in mehreren Abhandlungen in den Abh. und Nachr. von der kgl. Ges. der Wissensch. zu Göttingen. Vergl. auch Math. Annalen, Bd. 63.

β beliebige Zahlen (ganze und gebrochene) des Körpers $k(\sqrt{m})$. Dann bilden die sämtlichen Zahlen:

$$\alpha + \beta\sqrt{\mu}, \tag{1}$$

einen Bereich K oder einen Zahlkörper in dem früher gebrauchten Sinn, indem offenbar die Summe und die Differenz, das Produkt und der Quotient zweier Zahlen von der Form (1) wieder von derselben Form ist.

Jede Zahl $\mathsf{A} = \alpha + \beta\sqrt{\mu}$ dieses Bereichs genügt einer quadratischen Gleichung von der Form:

$$X^2 - 2\alpha X + \alpha^2 - \beta^2\mu = 0,$$

deren Koeffizienten dem Körper $k(\sqrt{m})$ angehören, und man nennt daher den Zahlkörper K *relativ quadratisch* in bezug auf $k(\sqrt{m})$. K heißt ein *Relativkörper* oder *Oberkörper* in bezug *auf* k; da andererseits der Körper K *alle Zahlen von* k enthält, so heißt k auch ein *Unterkörper* von K. Der Körper K ist dem quadratischen Körper $k(\sqrt{m})$ so übergeordnet, wie dieser dem Bereich der rationalen Zahlen.

Im folgenden sollen die Zahlen des Relativkörpers K mit *großen* griechischen Buchstaben bezeichnet werden, die Zahlen des Unter- oder Grundkörpers wie bisher mit den kleinen griechischen Buchstaben. Auch jetzt haben wir es i. a. nur mit den weiter unten definierten *ganzen* Zahlen des Relativkörpers zu tun, für welche diese Bezeichnung speziell gelten soll.

Zwei Zahlen $\alpha + \beta\sqrt{\mu}$ und $\alpha - \beta\sqrt{\mu}$, welche sich nur durch das Vorzeichen von $\sqrt{\mu}$ unterscheiden, heißen *relativ konjugiert*, und man pflegt zu sagen, daß die zweite Zahl aus der ersten durch die Substitution $S\,(\sqrt{\mu} : -\sqrt{\mu})$ hervorgehe. Analog wie früher mögen relativ konjugierte Zahlen durch denselben Buchstaben bezeichnet und durch ein beigesetztes S als A, $S(\mathsf{A})$ usw. unterschieden werden. Ferner sollen A und $s(\mathsf{A})$ zwei Zahlen sein, die durch Ersetzung von $\sqrt{m}$ durch $-\sqrt{m}$, d. h. durch die Substitution $s(\sqrt{m} : -\sqrt{m})$ aus- auseinander hervorgehen.

Eine beliebige Zahl aus K genügt einer Gleichung vom vierten Grad mit *rationalen* Koeffizienten. Es ist mithin absolut genommen K ein (spezieller) Zahlkörper vierten Grades. Alle Zahlen desselben A usw. sind rational durch $\mathsf{B} = \sqrt{\mu} + \sqrt{m}$ darstellbar in der folgenden Form:

$$\mathsf{A} = a + a_1\mathsf{B} + a_2\mathsf{B}^2 + a_3\mathsf{B}^3,$$

wobei a, a_1, a_2, a_3 rationale, i. a. gebrochene Zahlen bedeuten. Die Zahl A befriedigt eine Gleichung vierten Grades mit rationalen Koeffizienten:

$$(x - \mathsf{A})(x - s(\mathsf{A}))(x - S(\mathsf{A}))(x - Ss(\mathsf{A})) = 0.$$

Eine Zahl A des Relativkörpers K heißt eine *ganze* Zahl, wenn sie einer Gleichung genügt:

$$x^2 + \alpha x + \beta = 0,$$

wo α, β nun *ganze* Zahlen aus $k(\sqrt{m})$ bezeichnen. Es genügt alsdann A einer Gleichung vierten Grades mit ganzen rationalen Koeffizienten a_1, a_2, a_3, a_4 von der Form:

$$x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0,$$

und es ist daher A auch eine ganze Zahl im Körper vierten Grades K. Man kann die Definition der ganzen Zahl aber auch so fassen, daß man sagt, die Zahl A ist ganz, wenn

$$\mathsf{A} + S(\mathsf{A}) \quad \text{und} \quad \mathsf{A} \cdot S(\mathsf{A})$$

ganze Zahlen des Unterkörpers sind.

Das Produkt $\mathsf{A} \cdot S(\mathsf{A})$ aus einer Zahl und ihrer relativ Konjugierten heißt die *Relativnorm* der Zahl A, und soll künftig mit $N_k(\mathsf{A})$ bezeichnet werden. Die Relativnorm einer *ganzen* Zahl A aus K ist stets eine ganze Zahl des Grundkörpers $k(\sqrt{m})$.

Die Relativnorm einer Zahl α des Unterkörpers k ist $N_k(\alpha) = \alpha^2$, da $S(\alpha) = \alpha$ wird.

Aus der Definition der ganzen Zahl folgert man nun zunächst wieder, daß jede ganze Zahl aus K, welche dem Unterkörper $k(\sqrt{m})$ angehört, zugleich eine ganze Zahl dieses letzteren Körpers ist, und daß jede ganze Zahl aus K, welche rational ist, auch ganz und rational ist. Ferner beweist man auf dieselbe Weise, wie es für kubische ganze Zahlen in Nr. 39, S. 246 geschah, die Richtigkeit der in dem folgenden Satz enthaltenen Rechnungsgesetze:

Satz. *Die Summe, die Differenz und das Produkt von zwei ganzen Zahlen aus K ist wieder eine ganze Zahl des Körpers.*[1])

Es wird somit auch die Differenz:

$$\Delta_k = \mathsf{A} - S(\mathsf{A}),$$

welche die *Relativdifferente* der Zahl A heißt, ganz, wenn A ganz ist.

1) Wegen der in dieser Nummer eingeführten Begriffe vergl. Hilbert, Bericht, Kap. V, S. 203 und Kap. XV, § 57, S. 277.

Von der größten Wichtigkeit ist noch der Begriff der *Relativdiskriminante* einer Zahl A, wie der Ausdruck:

$$D_k(\mathsf{A}) = (\mathsf{A} - S(\mathsf{A}))^2$$

genannt wird. Die Relativdiskriminante einer Zahl A kann auch aufgefaßt werden als die negative Relativnorm der Relativdifferente von A, indem die Gleichung gilt:

$$D_k(\mathsf{A}) = - N_k(\Delta_k).$$

49. Basis des Relativkörpers.

Jede Zahl des Körpers $K(\sqrt{\mu})$ ist darstellbar in der Form:

$$\frac{\alpha + \beta\sqrt{\mu}}{\gamma},$$

wo nun α, β, γ ganze Zahlen des Körpers k sind. Es läßt sich nach den analogen Untersuchungen für die quadratischen und kubischen Körper vermuten, daß im Körper K unendlich viele Systeme von je vier ganzen Zahlen von der Besonderheit existieren, daß *jede ganze* Zahl aus K sich als lineare Kombination dieser vier Zahlen mit ganzen rationalen Koeffizienten darstellen läßt.

Zunächst bemerkt man, daß alle ganzen Zahlen aus K in zwei Klassen zerfallen: 1.) ganze Zahlen, die in K liegen, aber nicht zugleich Zahlen von k sind, und 2.) solche, die zugleich ganze Zahlen von k sind. Die letzteren lassen sich in der Form

$$x + y\omega$$

darstellen, wo x, y ganze rationale Zahlen und 1, ω eine Basis in k bezeichnen. Wir brauchen uns daher nur noch mit der Darstellung der ganzen Zahlen

$$\frac{\alpha + \beta\sqrt{\mu}}{\gamma}$$

zu beschäftigen, bei denen $\beta \neq 0$ ist.

Falls α, β, γ frei von allen unnötigen gemeinsamen Idealfaktoren angenommen werden, so findet man durch eine Überlegung, wie sie auch in Nr. 6, S. 21 ff. zur Anwendung kam, daß der Nenner γ einer ganzen Zahl als Primfaktoren nur enthalten kann: 1.) solche Primideale, welche in μ mindestens zur zweiten Potenz aufgehen und 2.) ev. Primfaktoren der Zahl 2. Wenn der Grundkörper die Klassenanzahl 1 besitzt, so enthält γ auch keine anderen ev. Primfaktoren als eben die unter 1.) resp. 2.) genannten; wenn aber $h > 1$ ist, so muß

man ev. α, β, γ durch ein bestimmtes akzessorisches Ideal teilbar voraussetzen.

Setzen wir fest, daß die überstrichenen Buchstaben $\bar{a}$ resp. $\bar{e}$ die größte ganze in $\frac{a}{2}$ und $\frac{e}{2}$ enthaltene Zahl vorstellen, daß also in sonst üblicher Bezeichnung $\bar{a} = \left[\frac{a}{2}\right]$ und $\bar{e} = \left[\frac{e}{2}\right]$ ist, so gelten jetzt die beiden folgenden Sätze, deren Beweis ganz nach dem Schema des Beweises in Nr. 6 geführt werden kann.

1. **Satz.** *Es besitze der Grundkörper $k(\sqrt{m})$ die Klassenanzahl $h = 1$; die Zahl 2 sei durch die Primfaktoren λ_1, λ_2 zu den Potenzen l_1 und l_2 teilbar: $2 = \lambda_1^{l_1}\lambda_2^{l_2}$; ferner sei die ganze Zahl μ in ihre Primfaktoren zerlegt:*

$$\mu = \lambda_1^{a_1}\lambda_2^{a_2}\pi_1^{e_1}\ldots\pi_r^{e_r},$$

und dabei mindestens einer der Exponenten a resp. e ungerade. Bezeichnen alsdann $g_1 \leqq l_1$ und $g_2 < l_2$ die größten positiven ganzen Zahlen, für welche die Kongruenz:

$$\mu \equiv \nu^2, \quad (\lambda_1^{2(g_1+\bar{a}_1)}\lambda_2^{2(g_2+\bar{a}_2)})$$

durch eine ganze Zahl ν des Grundkörpers befriedigt werden kann, und ist ν speziell eine solche Lösung dieser Kongruenz, daß

$$\nu = \pi_1^{\bar{e}_1}\ldots\pi_r^{\bar{e}_r}\nu_1$$

gesetzt werden kann[1]*), so ist:*

$$\Omega = \frac{\nu+\sqrt{\mu}}{\lambda_1^{g_1+\bar{a}_1}\lambda_2^{g_2+\bar{a}_2}\pi_1^{\bar{e}_1}\ldots\pi_r^{\bar{e}_r}} = \frac{\nu+\sqrt{\mu}}{\gamma}$$

eine ganze Zahl des Körpers $K(\sqrt{\mu})$ und die vier Zahlen:

$$1, \quad \omega, \quad \Omega, \quad \omega\Omega$$

bilden eine Basis des Relativkörpers.

Unter der Voraussetzung $h = 1$ ist also jede ganze Zahl des Körpers darstellbar in der Form

$$\frac{\alpha+\beta\sqrt{\mu}}{\gamma},$$

wo γ die in dem vorhergehenden Satz angegebene Bedeutung hat und wo α, β ganze Zahlen aus k sind.

---

1) Diese Voraussetzung darf man offenbar stets machen. Denn bedeutet ν irgend eine ganze Zahl, so kann man ν_1 stets so bestimmen, daß die Kongruenz erfüllbar ist: $\nu \equiv \pi_1^{\bar{e}_1}\ldots\pi_r^{\bar{e}_r}\nu_1$, $(\lambda_1^{2(g_1+\bar{a}_1)}\lambda_2^{2(g_2+\bar{a}_2)})$, da ja $\pi_1, \ldots \pi_r$ zu 2 prim sind.

Es ist vielleicht nicht überflüssig, darauf hinzuweisen, daß nur dann g_1 bez. $g_2 > 0$ sein kann, wenn a_1 bez. a_2 gerade Zahlen sind, und daß ferner ν notwendig durch $\lambda_1^{a_1}\lambda_2^{a_2}$ teilbar ist. Sollte $g_1 = g_2 = 0$ sein, so vereinfacht sich also Ω auf die Form $\frac{\sqrt{\mu}}{\gamma}$.

2. Satz. *Es besitze der Grundkörper $k(\sqrt{m})$ die Klassenanzahl $h > 1$, und es sei:*

$$(2) = \mathfrak{l}_1^{h}\mathfrak{l}_2^{h},$$

ferner:

$$(\mu) = \mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}\mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_r^{e_r}.$$

Wenn alsdann die Kongruenz:

$$\mu \equiv \nu^2, \quad \left(\mathfrak{l}_1^{2(g_1+\bar{a}_1)}\mathfrak{l}_2^{2(g_2+\bar{a}_2)}\right)$$

durch eine ganze Zahl des Grundkörpers befriedigt werden kann und $\mathfrak{b} = (\beta_1, \beta_2)$ ein Ideal bezeichnet von der Eigenschaft, daß $\mathfrak{b}$ prim zu $\mathfrak{l}_1$ und $\mathfrak{l}_2$ ist und daß

$$\mathfrak{l}_1^{g_1+\bar{a}_1}\mathfrak{l}_2^{g_2+\bar{a}_2}\mathfrak{p}_1^{\bar{e}_1}\ldots\mathfrak{p}_r^{\bar{e}_r}\,\mathfrak{b} = (\gamma)$$

ein Hauptideal wird, wenn schließlich wieder ν so gewählt ist, was nach den Sätzen über lineare Kongruenzen stets möglich ist, daß das Hauptideal

$$(\nu) = \mathfrak{p}_1^{\bar{e}_1}\ldots\mathfrak{p}_r^{\bar{e}_r}\cdot\mathfrak{n}$$

wird, so sind stets:

$$\Omega_1 = \beta_1\,\frac{\nu+\sqrt{\mu}}{\gamma}, \quad \Omega_2 = \beta_2\,\frac{\nu+\sqrt{\mu}}{\gamma}$$

ganze Zahlen des Körpers $K(\sqrt{\mu})$ und die vier Zahlen:

$$1, \ \omega, \ \Omega_1, \ \Omega_2$$

bilden eine Basis des Relativkörpers.

Die Wahl des Nenners γ ist nach diesem Satze noch in beschränktem Maße willkürlich, je nach der Wahl von $\mathfrak{b}$, doch läßt sich jede ganze Zahl des Körpers auf eine solche mit dem speziellen Nenner γ zurückführen. Denn nimmt man z. B.

$$\Omega = \beta\,\frac{\sigma+\sqrt{\mu}}{\gamma_1},$$

wo

$$\frac{\gamma}{\gamma_1} = \frac{\mathfrak{b}}{\mathfrak{b}_1}$$

ist, und multipliziert man Zähler und Nenner von Ω mit $\frac{\mathfrak{b}}{\mathfrak{b}_1}$, so wird:

$$\mathfrak{Q} = \frac{\varrho - \tau\sqrt{\mu}}{\gamma_1 \frac{\mathfrak{b}}{\mathfrak{b}_1}} = \frac{\varrho + \tau\sqrt{\mu}}{\gamma},$$

weil ja β nach seiner Konstruktion teilbar ist durch $\mathfrak{b}_1$.

Aus jeder Basis lassen sich unendlich viele Quadrupel von Zahlen ableiten, die ebenfalls eine Basis des Relativkörpers bilden; irgend zwei dieser Quadrupel hängen durch eine Substitution mit ganzzahligen, dem Körper $k(\sqrt{m})$ angehören Koeffizienten von der Determinante ± 1 zusammen.

Zu dem zweiten Satz ist noch zu bemerken: das dort eingeführte Ideal $\mathfrak{b}$ könnte auch so gewählt werden, daß es nur die Ideale $\mathfrak{l}_1$, $\mathfrak{l}_2$, $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ als Primfaktoren enthält, so daß γ in 4μ aufgeht. Der zweite Satz enthält den ersten Satz als speziellen Fall, jedoch sind beide Sätze getrennt aufgeführt, da der erste Satz wohl unmittelbarer verständlich ist.

50. Ideale des Relativkörpers.

Die Definitionen des Ideals und der Gleichheit zweier Ideale für die Körper zweiten und dritten Grades lassen sich wörtlich auf den Körper K übertragen. Jedes Ideal $\mathfrak{j} = (\iota, \iota_1)$ des Unterkörpers ist auch ein Ideal $\mathfrak{J}$ des Relativkörpers, dessen sämtliche Zahlen eben nur lineare Kombinationen von ι, ι_1 mit ganzen Zahlen des Relativkörpers sind, und es ist $\mathfrak{J} = \mathfrak{j}$. Umgekehrt ist ein Ideal des Relativkörpers $\mathfrak{J}$ zugleich ein Ideal des Unterkörpers, wenn $\mathfrak{J}$ sich durch ein System von Zahlen des Unterkörpers ι, ι_1 darstellen läßt. Es ist aber selbstverständlich nicht jedes Ideal $\mathfrak{J}$ des Relativkörpers gleichzeitig ein Ideal des Grundkörpers.

Die Definition des *Hauptideals* bleibt dieselbe wie früher.

Nimmt man in allen Zahlen eines Ideals $\mathfrak{J}$ die Substitution $S(\sqrt{\mu}: -\sqrt{\mu})$ vor, so erhält man wieder ein Ideal, welches mit $S(\mathfrak{J})$ bezeichnet werden kann und welches das zu $\mathfrak{J}$ *relativ konjugierte Ideal* heißt. Ein Ideal $\mathfrak{J}$, das seinem relativ konjugierten Ideal gleich ist und welches kein Ideal aus k als Faktor enthält, bezeichnet man als *ambiges* Ideal.

Indem man alle Zahlen eines Ideals durch eine Basis 1, ω, $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ ausdrückt und die Überlegungen wiederholt, welche an andern Stellen zur Herstellung einer *Basis des Ideals* benützt wurden, findet man, daß jedes Ideal $\mathfrak{J}$ sich in der Form anschreiben läßt:

$$\mathfrak{J} = (i, \iota, \mathfrak{l}, \mathfrak{l}_1),$$

wo $i, \iota, \mathfrak{l}, \mathfrak{l}_1$ eine Basis des Ideals bedeuten.

Bezüglich der Definitionen des Produkts zweier Ideale, der Norm eines Ideals, und des Beweises der eindeutigen Zerlegbarkeit eines Ideals in Primfaktoren kann ich mich mit dem einfachen Verweis auf die Nrn. 11 und 43, 44 begnügen.

Bezeichnet dann $n(\mathfrak{j})$ die Norm eines Ideals $\mathfrak{j}$ aus k, und zwar nur in bezug auf diesen Grundkörper k selbst, und ist ferner $N(\mathfrak{j})$ die Norm desselben Ideals für den Oberkörper K, so gilt die Gleichung:

$$N(\mathfrak{j}) = n(\mathfrak{j})^2.$$

Ist $\mathfrak{j} = (i, i_0 + i_1\omega)$ ein Ideal aus k, so bilden für dasselbe, als Ideal aus $K(\sqrt{\mu})$ vier Zahlen von der Form: i, $i_0 + i_1\omega$, $a_1 + b_1\omega + \frac{i}{g}\Omega_1$, $a_2 + b_2\omega + c_2 i_1 \Omega_1 + g i_1 \Omega_2$ eine Basis. Darum ist $N(\mathfrak{j}) = (i i_1)^2 = n(\mathfrak{j})^2$.

Wäre z. B. (und dieser Fall wird später auftreten) $\mathfrak{p}$ ein Ideal, das dem Grundkörper angehört, $\mathfrak{P}$ ein Ideal aus $K(\sqrt{\mu})$ von der Beschaffenheit, daß $\mathfrak{p} = \mathfrak{P}^2$ wird, so folgt:

$$(n(\mathfrak{p}))^2 = N(\mathfrak{p}) = N(\mathfrak{P}^2) = N(\mathfrak{P})^2,$$

also schließlich, da $n(\mathfrak{p})$ und $N(\mathfrak{P})$ ganze rationale positive Zahlen bedeuten:

$$n(\mathfrak{p}) = N(\mathfrak{P}).$$

Eine Erweiterung des Begriffs Norm eines Ideals ist der Begriff der *Relativnorm eines Ideals* $\mathfrak{J}$, als welche man das Produkt:

$$N_k(\mathfrak{J}) = \mathfrak{J} \cdot S(\mathfrak{J})$$

bezeichnet.

Die Relativnorm eines beliebigen Ideals $\mathfrak{J}$ aus K ist stets ein Ideal des Grundkörpers.

In der Tat, es bezeichne

$$\mathfrak{J} = (i, \iota, \mathfrak{l}, \mathfrak{l}_1)$$

ein Ideal aus dem Relativkörper, dargestellt durch seine Basis. Vereinigt man nun alle Zahlen aus dem Ideal $\mathfrak{J} \cdot S(\mathfrak{J})$, welche im Grundkörper liegen, zu einem Ideal $\mathfrak{j}$:

$$\mathfrak{j} = (i^2, i\iota, \iota^2, \mathfrak{l}S(\mathfrak{l}), \mathfrak{l}_1 S(\mathfrak{l}_1), \mathfrak{l}S\mathfrak{l}_1 + \mathfrak{l}_1 S\mathfrak{l}, \mathfrak{l}\mathfrak{l}_1 S(\mathfrak{l}\mathfrak{l}_1) \ldots),$$

das ebenfalls dem Grundkörper angehört, so ist $\mathfrak{j}$ identisch mit $\mathfrak{J} \cdot S(\mathfrak{J})$.

Denn da z. B.

$$\mathfrak{l}S(\mathfrak{l}_1) + \mathfrak{l}_1 S(\mathfrak{l}) \equiv 0, \ (\mathfrak{j}) \tag{1}$$

$$\mathfrak{l}S(\mathfrak{l}) \cdot \mathfrak{l}_1 S(\mathfrak{l}_1) \equiv 0, \ (\mathfrak{j}^2) \tag{2}$$

ist, so folgt, daß auch die Kongruenzen gelten:

$$\mathfrak{l}S(\mathfrak{l}_1) \equiv 0, \ (\mathfrak{j}) \quad \text{und} \quad \mathfrak{l}_1 S(\mathfrak{l}) \equiv 0, \ (\mathfrak{j}).$$

Wäre nämlich $\mathfrak{P}$ ein Teiler von $\mathfrak{j}$, und $\mathsf{l} \cdot S(\mathsf{l}_1)$ prim zu $\mathfrak{P}$, so ist nach Kongruenz (1) auch $\mathsf{l}_1 \cdot S(\mathsf{l})$ prim $\mathfrak{P}$, daher könnte $\mathsf{l} \cdot S(\mathsf{l}_1) \cdot \mathsf{l}_1 S(\mathsf{l})$ nicht durch $\mathfrak{P}^2$ teilbar sein, wie die Kongruenz (2) verlangt. Ebenso folgt, daß auch $i S(\mathsf{l})$, $i\mathsf{l}$ usw. durch $\mathfrak{j}$ teilbar sind oder es ist $\mathfrak{j} = N_k(\mathfrak{J})$, wie der Satz behauptet.

Hieraus folgt speziell, daß das Quadrat jedes ambigen Ideals $\mathfrak{A}$ stets ein Ideal des Grundkörpers k ist.

[Anmerkung. Den Beweis für die eindeutige Zerlegbarkeit der Ideale in Primideale kann man, statt nach dem Vorbild von Nr. 13 oder Nr. 43, S. 265 ff., auch anders führen. Man beweist zunächst den letzten Satz: das Quadrat eines ambigen Ideals ist stets ein Ideal des Grundkörpers; und benützt alsdann die Fundamentalsätze, welche für diesen Grundkörper gelten.]

Für die Kenntnis des Relativkörpers sind nun noch zwei neue Begriffe besonders wichtig: die Begriffe der *Relativdifferente* und der *Relativdiskriminante* des Körpers.

Die erstere ist der größte gemeinsame Teiler der Relativdifferenten aller ganzen Zahlen des Körpers:

$$\mathfrak{D}_k = (\mathsf{A} - S(\mathsf{A}),\ \mathsf{A}_1 - S(\mathsf{A}_1),\ \ldots);$$

die Relativdiskriminante ist:

$$\mathfrak{d} = \mathfrak{D}_k^2 = (\mathsf{A} - S(\mathsf{A}),\ \mathsf{A}_1 - S(\mathsf{A}_1),\ \ldots)^2.$$

Die Relativdifferente ist ein Ideal aus K, die Relativdiskriminante aber ein Ideal des Grundkörpers, da ja die Gleichheit

$$\mathfrak{d} = N_k(\mathfrak{D}_k)$$

gilt.

51. Die Teiler der Relativdiskriminante.

Satz. *Wenn $\mathfrak{p}$ ein in (2) nicht aufgehendes Primideal des Grundkörpers k ist, welches in (μ) genau zur e^{ten} Potenz aufgeht, so ist die Relativdiskriminante des Oberkörpers $K(\sqrt{\mu})$ dann und nur dann durch $\mathfrak{p}^1$ teilbar, falls e ungerade ist.*

Wenn ferner im Grundkörper $k(\sqrt{m})$ die Zerlegung $(2) = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2}$ gilt, und wenn $\mathfrak{l}_i$ in (μ) zur a_i^{ten} Potenz enthalten ist, so ist die Relativdiskriminante von $K(\sqrt{\mu})$ dann und nur dann prim zu $\mathfrak{l}_i$, wenn im Grundkörper eine ganze Zahl ν existiert, so daß

$$\mu \equiv \nu^2, \quad (\mathfrak{l}_i^{2l_i + a_i})$$

ausfällt.[1])

1) Vergl. Hilbert, Math. Ann., Bd. 51, S. 5 ff.

Beweis. Nach der oben aufgestellten Definition der Relativdiskriminante ist

$$\mathfrak{d} = (\mathsf{A} - S(\mathsf{A}),\ \mathsf{A}_1 - S(\mathsf{A}_1), \ldots)^2.$$

Wenn nun hierin die Zahlen A_i durch die Basis (vergl. Nr. 49 S. 298 ff.) ausgedrückt werden, so folgt:

$$\mathfrak{d} = \left(\frac{2\beta_1\sqrt{\mu}}{\gamma},\ \frac{2\beta_2\sqrt{\mu}}{\gamma},\ \frac{2(x\beta_1 + y\beta_2)\sqrt{\mu}}{\gamma},\ \ldots\right)^2$$

oder

$$\mathfrak{d}\cdot(\gamma^2) = (\mu)\cdot(2)^2(\beta_1,\ \beta_2)^2 = (\mu)(2)^2\cdot\mathfrak{b}^2,$$

also nach Einsetzung der Primfaktoren:

$$\mathfrak{d} = \frac{\mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}\mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_r^{e_r}\cdot\mathfrak{l}_1^{2l_1}\mathfrak{l}_2^{2l_2}\mathfrak{b}^2}{\mathfrak{l}_1^{2g_1+2\bar{a}_1}\mathfrak{l}_2^{2g_2+2\bar{a}_2}\mathfrak{p}_1^{2\bar{e}_1}\ldots\mathfrak{p}_r^{2\bar{e}_r}\mathfrak{b}^2}.$$

Aus dieser Darstellung der Relativdiskriminante folgt die Richtigkeit des Satzes unmittelbar.

Ist e_i gerade, also $\frac{e_i}{2} = \bar{e}_i$, so ist $\mathfrak{d}$ prim zu $\mathfrak{p}_i$; ist dagegen e_i ungerade, so wird $e_i = 2\bar{e}_i + 1$ und $\mathfrak{d}$ enthält den Faktor $\mathfrak{p}_i^1$, womit der erste Teil des Satzes bewiesen ist.

Gilt ferner die Kongruenz:

$$\mu \equiv \nu^2,\ (\mathfrak{l}_i^{2l_i + a_i}),$$

so muß zunächst a_i gerade sein, und man hat in dem Ausdruck für γ die Zahl $g_i = l_i$ zu setzen (vergl. S. 299). Alsdann enthält der Zähler und Nenner des Ausdrucks $\mathfrak{d}$ die Potenz $\mathfrak{l}_i^{2l_i + a_i}$ und es ist $\mathfrak{d}$ prim zu $\mathfrak{l}_i$. Ist indessen a_i ungerade, oder gilt die Kongruenz:

$$\mu \equiv \nu^2,\ (\mathfrak{l}_i^{2(g_i + \bar{a}_i)})$$

nur für ein $g_i < l_i$, so enthält $\mathfrak{d}$ notwendig den Faktor $\mathfrak{l}_i$ und damit ist auch der zweite Teil des Satzes bewiesen.

Durch eine Zusammenfassung der Resultate für $\mathfrak{l}_1$ und $\mathfrak{l}_2$ ergibt sich aus dem zweiten Teil des vorhergehenden Satzes:

Satz. *Wenn* (μ) *prim ist zu* (2) *und es gilt die Kongruenz:*

$$\mu \equiv \nu^2,\ (2^2),$$

so ist die Relativdiskriminante $\mathfrak{d}$ *des Körpers* $K(\sqrt{\mu})$ *auch ihrerseits prim zu dem Ideal* (2).

52. Die Primideale des Relativkörpers.

Die Entscheidung darüber, wann ein Primideal $\mathfrak{p}$ des Grundkörpers k im Relativkörper K zerlegbar ist oder nicht, ist in den folgenden Sätzen ausgesprochen (Hilbert, l. c., S. 8 f.).

1. Satz. *Wenn $\mathfrak{p}$ ein Primideal des Körpers k bezeichnet, welches relativ prim ist zu den Zahlen μ und 2, so ist $\mathfrak{p}$ dann und nur dann im Relativkörper K in das Produkt zweier voneinander verschiedenen Primideale $\mathfrak{P}$, $\mathfrak{P}_1$ zerlegbar, wenn μ quadratischer Rest nach $\mathfrak{p}$ ist, d. h. wenn eine ganze Zahl α in k existiert, so daß*

$$\mu \equiv \alpha^2, \ (\mathfrak{p})$$

ausfällt.

Beweis. Wenn die Kongruenz erfüllt ist:

$$\mu \equiv \alpha^2, \ (\mathfrak{p}),$$

so setze man

$$\mathfrak{P} = (\mathfrak{p}, \ \alpha + \sqrt{\mu}), \quad \mathfrak{P}_1 = S(\mathfrak{P}) = (\mathfrak{p}, \ \alpha - \sqrt{\mu}),$$

dann sind $\mathfrak{P}$ und $S(\mathfrak{P})$ zwei voneinander verschiedene Ideale, da wegen der Voraussetzung über $\mathfrak{p}$ und μ auch α prim ist zu $\mathfrak{p}$ und folglich:

$$(\mathfrak{p}, \ \alpha + \sqrt{\mu}, \ \alpha - \sqrt{\mu}, \ 2\alpha, \ 2\sqrt{\mu}, \ 2\mu) = (1)$$

wird. Ferner gilt für $\mathfrak{p}$ die Gleichung:

$$\mathfrak{p} = \mathfrak{P} \cdot S(\mathfrak{P}) = \left(\mathfrak{p}^2, \ \mathfrak{p}(\alpha + \sqrt{\mu}), \ \mathfrak{p}(\alpha - \sqrt{\mu}), \ \mu - \alpha^2, \ 2\mathfrak{p}\alpha, \ 2\mathfrak{p}\mu, \ \mathfrak{p} \ldots\right),$$

womit ein Teil der Behauptung des Satzes bewiesen ist.

Setzt man nun umgekehrt voraus, daß $\mathfrak{p}$ ein Primideal des Körpers k ist, welches im Relativkörper K in ein Produkt zweier Ideale zerfällt, nach der Gleichung:

$$\mathfrak{p} = \mathfrak{P} \cdot \mathfrak{P}_1,$$

so folgt zunächst aus der Gleichheit der Relativnormen der beiden Seiten der Gleichung: $\mathfrak{p}^2 = \mathfrak{P} S(\mathfrak{P}) \cdot \mathfrak{P}_1 S(\mathfrak{P}_1)$, daß $\mathfrak{P}_1 = S(\mathfrak{P})$ zu nehmen ist, weil ja nur eine einzige Zerlegung von $\mathfrak{p}$ existiert. Bedeutet alsdann A eine Zahl aus $\mathfrak{P}$, welche dem Relativkörper angehört, dann wird notwendig:

$$N_k(\mathsf{A}) \equiv 0, \ (\mathfrak{p}).$$

Ist etwa $\mathsf{A} = \frac{\alpha + \beta\sqrt{\mu}}{\gamma}$, so ist um so mehr

$$N_k(\alpha + \beta\sqrt{\mu}) \equiv 0, \ (\mathfrak{p}).$$

Es sei zunächst (γ) nicht durch $\mathfrak{p}$ teilbar. Wäre $\beta \equiv 0, \ (\mathfrak{p})$, so müßte auch $\alpha \equiv 0, \ (\mathfrak{p})$ sein, dann würden α und β selbst dem Ideale $\mathfrak{p}$ angehören, deshalb dürfen wir von dieser Annahme absehen. Wenn aber β prim zu $\mathfrak{p}$ ist, so gibt es, wie gezeigt wurde, eine ganze Zahl ξ in k, für welche

$$\beta\xi \equiv \pm 1, \ (\mathfrak{p})$$

wird, und es ist ξ ebenfalls prim zu $\mathfrak{p}$, daher ergibt sich aus:

$$\alpha^2 - \beta^2 \mu \equiv 0, \ (\mathfrak{p}),$$

auch:

$$(\xi \alpha)^2 - \mu \equiv 0, \ (\mathfrak{p}),$$

oder es ist μ quadratischer Rest nach $\mathfrak{p}$. Falls nun weiter $\mathfrak{p}$ in γ aufgeht, aber prim ist zu β, so bleibt die bisherige Überlegung und das Resultat richtig. Ist aber γ durch $\mathfrak{p}^{e_1}$ und ebenso α und β durch $\mathfrak{p}^e$ teilbar, $e_1 \geqq e$, so sei $\mathfrak{s}$ ein zu $\mathfrak{p}^e$ relativ primes äquivalentes Ideal, und $\frac{\mathfrak{p}^e}{\mathfrak{s}} = \frac{\pi}{\sigma}$, wo π genau durch die e^{te} Potenz von $\mathfrak{p}$ teilbar sein soll; dann setze man $\alpha = \frac{\pi}{\sigma} \alpha^*$ und $\beta = \frac{\pi}{\sigma} \beta^*$, alsdann sind α^* und β^* prim zu $\mathfrak{p}$, und es muß nun $\alpha^{*2} - \beta^{*2} \mu \equiv 0, \ (\mathfrak{p})$ sein, usw.

Dies ist also wieder dasselbe Resultat wie in dem vorigen Fall und damit ist der Satz vollständig bewiesen.

Nach einem ganz analogen Verfahren, wie wir es eben verwendet haben und unter Benutzung der früher aufgestellten Basis für den Relativkörper zeigt man die folgende Tatsache:

2. Satz. *Wenn $\mathfrak{l}_i$ ein Primideal des Körpers $k(\sqrt{m})$ bezeichnet, dessen l_i^{te} Potenz in 2 aufgeht, wenn ferner μ prim zu $\mathfrak{l}_i$ und kongruent dem Quadrat einer ganzen Zahl aus k nach $\mathfrak{l}_i^{2 l_i}$ ist, so daß also die Relativdiskriminante von $K(\sqrt{\mu})$ zu $\mathfrak{l}_i$ prim ausfällt, so ist $\mathfrak{l}_i$ im Relativkörper $K(\sqrt{\mu})$ dann und nur dann in zwei voneinander verschiedene Primideale zerlegbar, wenn es eine ganze Zahl α in k gibt, für welche die Kongruenz gilt:*

$$\mu \equiv \alpha^2, \ (\mathfrak{l}_i^{2 l_i + 1}).$$

Die beiden vorstehenden Sätze geben eine Entscheidung über die Zerlegbarkeit derjenigen Primideale aus k, welche *nicht* in der Relativdiskriminante enthalten sind. Zur Ergänzung der vorhergehenden Sätze gehören daher die beiden folgenden Sätze:

3. Satz. *Die Relativdifferente des Relativkörpers $K(\sqrt{\mu})$ ist durch alle und nur diejenigen Primideale teilbar, welche ambig sind.*

Beweis. Die Relativdifferente $\mathfrak{D}_k$ ist selbst ein Ideal, das seinem relativkonjugierten Ideal gleich ist, und kann nur durch ambige Primideale oder ev. Primideale aus k teilbar sein. Setzt man nämlich:

$$\mathfrak{D}_k = \mathfrak{P} \cdot \mathfrak{P}_1 \cdot \mathfrak{P}_2 \ldots \mathfrak{P}_r$$

und nimmt $\mathfrak{P}, \mathfrak{P}_1, \ldots \mathfrak{P}_r$ als Primideale aus K an, so ist doch auch wegen $\mathfrak{D}_k = S(\mathfrak{D}_k)$:

$$\mathfrak{D}_k = S(\mathfrak{P}) S(\mathfrak{P}_1) \ldots S(\mathfrak{P}_r).$$

Es muß also entweder $\mathfrak{P} = S(\mathfrak{P})$ usw. sein, oder $\mathfrak{P} = S(\mathfrak{P}_i)$. Wenn

daher zwei relativkonjugierte Ideale $\mathfrak{P}_a$ und $S(\mathfrak{P}_a)$ verschieden wären, so müßte $\mathfrak{D}_k$ durch das Idealprodukt $\mathfrak{P}_a S(\mathfrak{P}_a)$ teilbar sein.

$\mathfrak{P}_a S(\mathfrak{P}_a) = N_k(\mathfrak{P}_a) = \mathfrak{p}$ ist aber ein Ideal des Grundkörpers k und kann jedenfalls dann nicht in $\mathfrak{D}_k$ aufgehen, wenn $\mathfrak{p}$ verschieden ist von $\mathfrak{l}_1, \mathfrak{l}_2$, d. h. wenn $\mathfrak{p}$ prim ist zu der Zahl 2. Es enthält nämlich die Relativdiskriminante $\mathfrak{d} = \mathfrak{D}_k^2 = (\mathsf{A} - S(\mathsf{A}), \mathsf{A}_1 - S(\mathsf{A}_1), \ldots)^2$ außer den ev. Faktoren der Zahl 2 nur solche Primideale $\mathfrak{p}$ des Grundkörpers, welche in μ zu ungerader Potenz enthalten sind, und zwar steckt dann $\mathfrak{p}$ genau zur Potenz 1 in $\mathfrak{d}$. Wenn nun schon $\mathfrak{D}_k$ durch ein Primideal $\mathfrak{p}$ teilbar wäre, so wäre $\mathfrak{d} = \mathfrak{D}_k^2$ durch $\mathfrak{p}^2$ teilbar, im Widerspruch zu der vorhergehenden Behauptung.

Enthält ferner die Relativdiskriminante $\mathfrak{d}$ ein Ideal $\mathfrak{l}_i$, das in der Zahl 2 aufgeht, so läßt sich zeigen, daß $\mathfrak{l}_i$ gleich dem Quadrat eines ambigen Primideals $\mathfrak{L}_i$ des Oberkörpers K wird, welches alsdann in der Relativdifferente enthalten ist.

Ist nämlich erstens $\mathfrak{l}_i$ zu ungerader Potenz in μ enthalten, dann wird offenbar $\mathfrak{l}_i = \left(\mathfrak{l}_i, \frac{\beta}{\gamma}\sqrt{\mu}\right)^2 = \mathfrak{L}_i^2$, und $\mathfrak{L}_i$ ist ein von (1) verschiedenes, ambiges Ideal des Oberkörpers. Steckt hingegen $\mathfrak{l}_i$ zu gerader Potenz a_i in μ und ist (mit der in Nr. 49 verwendeten Bezeichnung) die Kongruenz:

$$\mu \equiv \nu^2, \ (\mathfrak{l}_i^{2g_i + a_i})$$

nur für eine Zahl $g_i < l_i$ erfüllt, so kann man die ganze Zahl

$$\mathsf{A} = \frac{\alpha + \beta\sqrt{\mu}}{\gamma}$$

derart bestimmen, daß $N_k(\mathsf{A})$ durch $\mathfrak{l}_i$ teilbar ist. Nach der Voraussetzung über die Zahl μ ist γ durch $\mathfrak{l}_i^{g_i + \bar{a}_i}$ und α durch $\mathfrak{l}_i^{\bar{a}_i}$ teilbar, und es bleibt in der Tat nur zu zeigen, daß α und β derart gewählt werden können, daß:

$$\alpha^2 - \beta^2\mu \equiv 0, \ (\mathfrak{l}_i^{2g_i + a_i + 1})$$

wird. Setzt man, analog wie im Beweis des ersten Satzes,

$$\mu = \frac{\lambda^2}{\sigma^2}\mu^* \quad \text{und} \quad \alpha = \frac{\lambda}{\sigma}\alpha^*,$$

wo λ genau durch die Potenz $\mathfrak{l}_i^{a_i/2}$ und keine höhere Potenz von $\mathfrak{l}_i$ teilbar und σ prim zu $\mathfrak{l}_i$ ist, während nun α^* und μ^* prim sind zu $\mathfrak{l}_i$, so hat man α^* und β so zu bestimmen, daß die Kongruenz:

$$\alpha^{*2} - \beta^2\mu^* \equiv 0, \ (\mathfrak{l}_i^{2g_i + 1}) \qquad (1)$$

befriedigt wird. Weil β prim ist zu $\mathfrak{l}_i$, so ist diese Kongruenz gleichwertig mit der weiteren:

$$\xi^2 - \mu^* \equiv 0, \ (\mathfrak{l}_i^{2g_i+1}), \tag{2}$$

wobei außerdem

$$\mu^* \equiv \nu^{*2}, \ (\mathfrak{l}_i^{2g_i}) \tag{3}$$

sein muß.

Wenn erstens das Ideal (2) im Unterkörper k Primideal ist, so ist in der Kongruenz (1): $g_1 = 0$ zu nehmen und es bleibt nachzuweisen, daß die Kongruenz

$$\xi^2 - \mu^* \equiv 0, \ (2)$$

stets eine Lösung besitzt.

Nun ist die Zahl 2 im Körper $k(\sqrt{m})$ nur dann unzerlegbar, wenn $m \equiv 5, (8)$ ist. Dann bilden $1, \omega = \frac{1+\sqrt{m}}{2}$ eine Basis des Grundkörpers, und wir dürfen

$$\xi = x + y\omega, \quad \mu^* = a + b\omega$$

setzen. Wegen:

$$\omega^2 = \frac{m-1}{4} + \omega, \quad \text{und} \quad \frac{m-1}{4} \equiv 1, \ (2)$$

wird nunmehr:

$$\xi^2 - \mu^* \equiv x^2 + y^2 - a + (y^2 - b)\omega \equiv 0, \ (2)$$

und diese Kongruenz ist stets in ganzen Zahlen x, y lösbar, weil die Kongruenzen

$$x^2 + y^2 - a \equiv 0, \ (2) \quad \text{und} \quad y^2 - b \equiv 0, \ (2)$$

unter allen Umständen lösbar sind.

Wenn zweitens die Zahl 2 im Unterkörper k zerlegbar ist, also entweder $(2) = \mathfrak{l}_1 \cdot \mathfrak{l}_2$ oder $(2) = \mathfrak{l}_1^2$ ausfällt, so hat man im ersten Fall zu entscheiden, ob die Kongruenz:

$$\xi^2 - \mu^* \equiv 0, \ (\mathfrak{l}_i^1), \tag{4}$$

und im zweiten Fall, ob die Kongruenz

$$\xi^2 - \mu^* \equiv 0, \ (\mathfrak{l}_1) \tag{5}$$

resp.

$$\xi^2 - \mu^* \equiv 0, \ (\mathfrak{l}_1^3) \tag{6}$$

lösbar ist.

Für jede dieser drei Möglichkeiten existiert aber eine Lösung. Wir beschäftigen uns zunächst mit der letzten Möglichkeit, d. h. mit der Kongruenz (6).

Die Kongruenz

$$\xi^2 - \mu^* \equiv 0, \ (\mathfrak{l}_1^2)$$

hat eine Lösung, denn aus der Voraussetzung:

$$\mu \equiv \nu^2, \ (\mathfrak{l}_1^{2+a_1}),$$

20*

folgt:

$$\mu^* \equiv \nu^{*2}, \ (\mathfrak{l}_1^2),$$

und zwar ist $\xi = \nu^*$.

Wenn nun nicht schon $\xi = \nu^*$ eine ganze Zahl des Körpers ist, für welche:

$$\xi^2 - \mu^* \equiv 0, \ (\mathfrak{l}_1^3)$$

ausfällt, so setze man

$$\xi_1 = \xi + \lambda x,$$

wo jetzt λ eine durch die erste Potenz von $\mathfrak{l}_1$, nicht aber durch $\mathfrak{l}_1^2$ teilbare Zahl sei.

Die Kongruenz

$$\xi_1^2 - \mu^* \equiv 0, \ (\mathfrak{l}_1^3)$$

ist alsdann gleichwertig mit der folgenden:

$$\frac{\xi^2 - \mu^*}{2} + x^2 \frac{\lambda^2}{2} \equiv 0, \ (\mathfrak{l}_1).$$

Da nun $\frac{\lambda^2}{2}$ prim ist zu $\mathfrak{l}_1$, so ist diese Kongruenz von genau derselben Form $\xi^2 - \mu^* \equiv 0$, $(\mathfrak{l}_1)$, von welcher auch die beiden noch zu untersuchenden Kongruenzen sind. Weil in diesen $n(\mathfrak{l}_i) = 2$ ist, so ist jede Zahl des Körpers kongruent einer ganzen rationalen zu 2 primen Zahl, und die Kongruenzen

$$\xi^2 - \mu \equiv 0, \ (\mathfrak{l}_i)$$

sind sicher lösbar, da die Kongruenz

$$x^2 - a \equiv 0, \ (2)$$

stets in ganzen rationalen Zahlen lösbar ist.

In allen eben betrachteten Fällen ist somit das Ideal $\mathfrak{l}_i$ im Relativkörper zerlegbar. Da ein Ideal

$$\left(\mathfrak{l}_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right) = \left(\mathfrak{l}_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}, 2\right)$$

stets auch die Zahl $\frac{\alpha - \beta\sqrt{\mu}}{\gamma}$ enthält, weil:

$$\left(\frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right) + \left(\frac{\alpha - \beta\sqrt{\mu}}{\gamma}\right) \equiv 0, \ (\mathfrak{l}_i)$$

und

$$\left(\frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right) - \left(\frac{\alpha - \beta\sqrt{\mu}}{\gamma}\right) \equiv 0, \ (\mathfrak{l}_i)$$

ist, so sind die sämtlichen aufgestellten Ideale ambig.

Hiermit ist der erste Teil unseres Satzes bewiesen.

Es bleibt noch zu beweisen, daß $\mathfrak{D}_k$ auch durch *alle* ambigen Ideale teilbar ist.

Zu diesem Zweck sei $\mathfrak{P}$ ein ambiges Ideal, und:

$$\mathfrak{p} = \mathfrak{P}^2,$$

bezeichnet dann n die Norm im Körper k, N die Norm im Körper K, so ist:

$$n(\mathfrak{p}) = n(\mathfrak{P}^2) = N(\mathfrak{P}).$$

Aus der Gleichheit der Normen der Ideale $\mathfrak{p}$ und $\mathfrak{P}$ folgt, daß das vollständige Restsystem nach $\mathfrak{P}$ durch lauter Zahlen des Unterkörpers k gebildet werden kann, indem ja eine Zahl, welche durch $\mathfrak{p}$ nicht teilbar ist, noch weniger durch $\mathfrak{P}$ teilbar sein kann. Folglich ist jede Zahl des Relativkörpers nach einem ambigen Ideal $\mathfrak{P}$ einer Zahl des Grundkörpers kongruent.

Aus:

$$\mathsf{A} \equiv \alpha, \ (\mathfrak{P})$$

folgt jedoch auch:

$$S(\mathsf{A}) \equiv \alpha, \ (\mathfrak{P}),$$

und daher wird:

$$\mathsf{A} - S(\mathsf{A}) \equiv 0, \ (\mathfrak{P}).$$

D. h. aber, *alle* Zahlen aus $\mathfrak{D}_k$ sind in $\mathfrak{P}$ enthalten, und daher ist $\mathfrak{D}_k$ teilbar durch $\mathfrak{P}$.

Der Satz 3 ist damit in allen Teilen bewiesen.

[Anmerkung. Aus dem Satz 3 folgt direkt auch die Bemerkung, daß ein Ideal $\mathfrak{l}_i$, welches nicht in der Relativdiskriminante aufgeht, im Relativkörper entweder gar nicht zerlegbar ist, oder in zwei voneinander verschiedene nicht ambige Primideale zerfällt.

In der Tat ist ja dann $\mu \equiv \nu^2$, $(\mathfrak{l}_i^{2l_i + a_i})$, und der Nenner γ der ganzen Zahl $\frac{\alpha + \beta\sqrt{\mu}}{\gamma}$ enthält den Faktor $\mathfrak{l}_i^{l_i + a_i}$, während β prim zu $\mathfrak{l}_i$ ist. Für den Fall, daß nun $\mathfrak{L}_i = \left(\mathfrak{l}_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}\right)$ ein Primfaktor von $\mathfrak{l}_i$ wird, ist notwendig

$$\left(\mathfrak{l}_i, \frac{\alpha + \beta\sqrt{\mu}}{\gamma}, \frac{\alpha - \beta\sqrt{\mu}}{\gamma}\right) = (1),$$

da $\left(\frac{2\beta\sqrt{\mu}}{\gamma}\right)^2$ prim zu $\mathfrak{l}_i$ ist.]

Es ist nun vollends leicht, aus dem dritten Satz den letzten Satz abzuleiten:

4. Satz. *Jedes Primideal des Grundkörpers k, welches in der Relativdiskriminante aufgeht, ist im Relativkörper gleich dem Quadrat eines ambigen Primideals. Umgekehrt ist jedes Primideal $\mathfrak{p}$ des Grundkörpers, welches durch das Quadrat eines Primideals aus dem Relativkörper teilbar ist, in der Relativdiskriminante $\mathfrak{d}$ enthalten.*

Beweis. Wenn $\mathfrak{P}$ ein ambiges Ideal des Relativkörpers ist, dessen Quadrat ein Primideal $\mathfrak{p}$ in k wird, so geht $\mathfrak{P}$ in der Relativdifferente $\mathfrak{D}_k$ und folglich $\mathfrak{P}^2 = \mathfrak{p}$ in der Relativdiskriminante auf, da ja $\mathfrak{d} = \mathfrak{D}_k^2$ ist. Es ist also jedes Ideal aus k, welches gleich dem Quadrat eines ambigen Primideals ist, in der Relativdiskriminante enthalten. Wenn ferner $\mathfrak{p} = \mathfrak{P}^2 \cdot \mathfrak{Q}$ ist, so ist auch $\mathfrak{p} = S(\mathfrak{P})^2 S(\mathfrak{Q})$, woraus zunächst folgt, daß $\mathfrak{P} = S(\mathfrak{P})$, $\mathfrak{Q} = S(\mathfrak{Q})$ sein muß; und da nun $\mathfrak{P} S(\mathfrak{P})$ in k liegt, so ist $\mathfrak{Q} = (1)$, $\mathfrak{p}$ also gleich dem Quadrat eines *ambigen* Ideals.

Geht ferner $\mathfrak{p}$ in der Relativdiskriminante $\mathfrak{d}$ auf, so geht $\mathfrak{p}$ in $\mathfrak{D}_k^2$ auf, es muß daher $\mathfrak{p} = \mathfrak{P}^2$ werden, da $\mathfrak{D}_k$ durch alle und nur durch ambige Primideale des Körpers $K(\sqrt{\mu})$ teilbar ist.

Die bisher entwickelten Sätze sind ganz allgemeiner Natur. Ich will nun an verschiedenen numerischen Beispielen die Grundgedanken weiterer allgemeinerer Untersuchungen (Vgl. Hilberts früher zitierte Abh.) erläutern. Die Sätze der folgenden Nummern sind insbesondere im Hinblick auf das schon in der Einleitung zu diesem Abschnitt gesteckte Ziel: Entwicklung und Beweis der einfachsten quadratischen Reziprozitätsgesetze für den Grundkörper $k(\sqrt{m})$, ausgewählt.

53. Die Relativdiskriminante eines Oberkörpers in bezug auf einen imaginären Grundkörper mit ungerader Klassenanzahl.

Über den quadratischen Unterkörper k soll für das Nächstfolgende vorausgesetzt werden (Hilbert, Math. Ann. 51 S. 27), daß er

1.) *ein imaginärer Körper ist;*

2.) *eine ungerade Klassenanzahl besitzt.*

Wegen der ersten Bedingung ist auch jeder Relativkörper $K(\sqrt{\mu})$ ein imaginärer Körper. Absolut betrachtet ist $K(\sqrt{\mu})$ ein Körper vierten Grades, der, wie seine sämtlichen konjugierten Körper, imaginär ist.

Es läßt sich alsdann mit Hilfe des Satzes von Minkowski, ähnlich wie in Nr. 47 S. 286ff., beweisen, daß im Körper $K(\sqrt{\mu})$ eine einzige, von ± 1 verschiedene, Grundeinheit E existiert, deren Norm eine Einheit im Grundkörper k ist also gleich ± 1, wenn wir von den Körpern $k(\sqrt{-1})$ und $k(\sqrt{-3})$ absehen.

Durch die zweite Bedingung ist der Grundkörper noch näher bestimmt. Aus den Sätzen über die Anzahl der Geschlechter in einem

quadratischen Zahlkörper k folgt, daß diese Anzahl für einen imaginären Körper stets gerade sein muß, wenn die Diskriminante des Körpers mehr als eine Primzahl enthält. Offenbar wird dann aber auch die Klassenanzahl gerade.

Die zweite Bedingung ist darum nur erfüllt, wenn m eine negative Primzahl von der Form $m \equiv 1$, (4), oder wenn $m = -1$, $m = -2$ ist.

Für den Körper $k(\sqrt{-3})$ existiert bereits eine Untersuchung des quadratischen Reziprozitätsgesetzes und der quadratischen Oberkörper von Herrn Dörrie, auf die ich einfach verweisen kann, ich will daher den Körper $k(\sqrt{-3})$ und den schon von Gauß behandelten Körper $k(\sqrt{-1})$ ausschließen und mich mit den übrigen Körpern beschäftigen, die den gestellten Bedingungen genügen. Die zu betrachtenden Körper sind alsdann: $k(\sqrt{-2})$, $\sqrt{-7}$, $\sqrt{-11}$, $\sqrt{-19}$, $\sqrt{-23}$, $\sqrt{-31}$, $\sqrt{-43}$, $\sqrt{-47}$ usw. usw., welche die resp. Klassenanzahlen 1, 1, 1, 1, 3, 3, 1, 5 usw. besitzen.

Nun ist es nicht schwer, zunächst folgende fundamentale Tatsache einzusehen:

Satz. *Wenn der Grundkörper $k(\sqrt{m})$ ein imaginärer Körper mit ungerader Klassenanzahl h ist, so ist für jeden Relativkörper $K(\sqrt{\mu})$ die Relativdiskriminante in bezug auf den Körper $k(\sqrt{m})$ verschieden von* ± 1.

Beweis. Nach den Sätzen über die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ enthält diese als Faktor: 1.) ein zu 2 primes Primideal $\mathfrak{p}$ aus k, wenn μ durch eine *ungerade* Potenz $\mathfrak{p}$ teilbar ist, 2.) das in (2) aufgehende Primideal $\mathfrak{l}$ aus k, falls μ durch $\mathfrak{l}^a$, das Ideal (2) durch $\mathfrak{l}^l$ teilbar ist, und die Kongruenz:

$$\mu \equiv \alpha^2, \quad (\mathfrak{l}^{2(l+a)})$$

nicht durch eine ganze Zahl α des Körpers k erfüllt werden kann.

Es ist schon früher darauf hingewiesen worden, daß diese letztere Kongruenz von vornherein nur dann erfüllbar ist, falls a gerade, $a = 2e$ ist. Angenommen nun, μ sei durch die Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{l}$ teilbar, so kann die Relativdiskriminante von $K(\sqrt{\mu})$ sicher nur dann zu allen diesen Faktoren prim ausfallen, wenn

$$(\mu) = \mathfrak{p}_1^{2e_1}\mathfrak{p}_2^{2e_2}\ldots\mathfrak{l}^{2e}$$

ist. Es wäre somit:

$$(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{l}^{e})^2 \sim 1;$$

da aber andererseits die Äquivalenz gilt:

$$(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{l}^{e})^h \sim 1,$$

wo h nach Voraussetzung eine ungerade Zahl ist, so müßte auch:

$$\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{l}^{e} \sim 1$$

ausfallen. Es wäre also $\mu = \varepsilon\nu^2$, das Produkt aus einer Einheit mit dem Quadrat einer ganzen Zahl ν.

Der Körper $K(\sqrt{\varepsilon\nu^2})$ stimmt aber überein mit dem Körper $K(\sqrt{\varepsilon})$. Um zu zeigen, daß die Relativdiskriminante von ± 1 verschieden ist, bleibt daher nach dem Schlußsatz von Nr. 51 S. 303 nur zu beweisen, daß in dem Körper $k(\sqrt{m})$ die Kongruenz

$$\varepsilon \equiv \alpha^2,\ (4)$$

nicht lösbar sein kann.

Da die Körper $k(\sqrt{-1})$, $k(\sqrt{-3})$ von der Betrachtung ausgeschlossen sind, so könnte nur $\varepsilon = -1$ sein, und man hat zu untersuchen, ob die Kongruenz

$$-1 \equiv (x + y\omega)^2,\ (4)$$

in ganzen rationalen Zahlen x, y lösbar ist.

Sei $\omega = \frac{1+\sqrt{m}}{2}$, so ist $\omega^2 = \frac{m-1}{4} + \omega$; man erhält also:

$$-1 \equiv x^2 + \frac{m-1}{4}y^2 + (2xy + y^2)\omega,\ (4),$$

d. h. es müßte gleichzeitig:

$$x^2 + \frac{m-1}{4}y^2 + 1 \equiv 0,\ (4)$$

und

$$2xy + y^2 \equiv 0,\ (4)$$

sein.

Wenn nun die zweite Kongruenz in ganzen Zahlen x, y lösbar ist, so ergibt sich y notwendig gerade, da andernfalls $2xy + y^2$ ungerade wäre. Sodann bliebe für x noch die Kongruenz:

$$x^2 + 1 \equiv 0,\ (4)$$

zu erfüllen, aber diese ist in ganzen Zahlen nicht lösbar. D. h. es kann keine Kongruenz von der Form $\varepsilon \equiv \alpha^2$, (4) bestehen.

Die Relativdiskriminante von $K(\sqrt{\varepsilon})$ ist also nicht prim zu 2 und daher verschieden von ± 1. Mithin ist der Satz bewiesen.

54. Einfache Fälle des Hilbertschen quadratischen Reziprozitätsgesetzes.

Satz. *Eine ganze oder gebrochene Zahl* B *des Relativkörpers* $K(\sqrt{\mu})$, *deren Relativnorm in bezug auf* k *gleich* $+1$ *ist, läßt sich als Quotient zweier relativ konjugierter ganzer Zahlen des Relativkörpers, d. h. in der Form* $\frac{\mathsf{A}}{S(\mathsf{A})}$ *darstellen.*

Beweis. Setzt man (vgl. Nr. 23 S. 108) unter der Voraussetzung $\mathsf{B} \neq -1$:

$$\mathsf{A}_1 = 1 + \mathsf{B},$$

so wird

$$S(\mathsf{A}_1) = 1 + S(\mathsf{B}) = \frac{1}{\mathsf{B}}(1 + \mathsf{B}),$$

und folglich wird einfach $\mathsf{B} = \frac{\mathsf{A}_1}{S(\mathsf{A}_1)}$. Indem man nun eine ganze rationale Zahl a so wählt, daß $a\mathsf{A}_1$ eine ganze Zahl ist, so wird auch $aS(\mathsf{A}_1)$ ganz. Es entspricht daher $\mathsf{A} = a\mathsf{A}_1$ den Anforderungen des Satzes, indem nun $\mathsf{B} = \frac{\mathsf{A}}{S(\mathsf{A})}$ ausfällt.

Mit einer Betrachtung, welche ohne weiteres auf beliebige Grundkörper anwendbar ist, kann man den Satz auch folgendermaßen beweisen:

Nach Voraussetzung ist $\mathsf{B} \cdot S(\mathsf{B}) = +1$; wenn nun θ eine ganze den Relativkörper bestimmende Zahl ist, so setze man:

$$\mathsf{B}_x = \frac{x + \theta}{x + S(\theta)}\mathsf{B}$$

und

$$\mathsf{A}_x = 1 + \mathsf{B}_x,$$

dann folgt zuerst $\mathsf{B}_x = \frac{\mathsf{A}_x}{S(\mathsf{A}_x)}$. Denn aus der letzten Gleichung ergibt sich unter Berücksichtigung der vorhergehenden:

$$\mathsf{B}_x S(\mathsf{A}_x) = \mathsf{B}_x(1 + S(\mathsf{B}_x)) = \mathsf{B}_x + 1 = \mathsf{A}_x.$$

Wählt man jetzt x gleich einer ganzen rationalen Zahl a derart, daß B_a nicht verschwindet, was offenbar stets möglich ist, dann kann man setzen:

$$\mathsf{A}_1 = \frac{\mathsf{A}_a}{a + \theta},$$

woraus

$$\mathsf{B} = \frac{\mathsf{A}_1}{S(\mathsf{A}_1)} = \frac{a + S(\theta)}{a + \theta}\,\frac{\mathsf{A}_a}{S(\mathsf{A}_a)} = \frac{a + S(\theta)}{a + \theta}\mathsf{B}_a$$

sich ergibt. Schreibt man alsdann $\mathsf{A}_1 = \frac{\mathsf{A}}{b}$, indem A eine ganze Zahl

des Relativkörpers und b eine ganze rationale Zahl bezeichnet, so ist auch

$$\mathsf{B} = \frac{\mathsf{A}}{S(\mathsf{A})},$$

und dies war zu beweisen.

Satz. *Wenn die Relativdiskriminante des Körpers* $K(\sqrt{\mu})$ *nur ein einziges Primideal* $\mathfrak{p}$ *aus* k *enthält, so ist die Relativnorm der Grundeinheit* E *in* K *gleich* -1.

Beweis. Es bezeichne E die Grundeinheit des Körpers $K(\sqrt{\mu})$. Angenommen, die Relativnorm dieser Grundeinheit sei $+1$, d. h. $N_k(\mathsf{E}) = +1$, so existiert nach dem vorhin bewiesenen Satz im Relativkörper K eine ganze Zahl A von der Beschaffenheit, daß:

$$\mathsf{E} = \frac{\mathsf{A}}{S(\mathsf{A})} \quad \text{oder} \quad \mathsf{A} = \mathsf{E}S(\mathsf{A})$$

ausfällt. Jeder Zahlenfaktor aus K, welcher in A aufgeht, muß daher auch in $S(\mathsf{A})$ aufgehen. Dies bedingt aber, daß A nur durch ambige Ideale aus K und außerdem ev. nur durch Ideale des Grundkörpers teilbar sein kann. Nach Voraussetzung enthält jedoch der Oberkörper $K(\sqrt{\mu})$ nur ein einziges ambiges Ideal $\mathfrak{P}$. Nun gibt es im Grundkörper ein Ideal $\mathfrak{m}$ von der Eigenschaft, daß $\mathfrak{m} \cdot \mathfrak{P} = \frac{\beta\sqrt{\mu}}{\gamma}$ wird, wo β und γ *ähnliche* Bedeutungen haben wie im Satz über die Basis des Körpers, S. 299; da ferner der imaginäre Grundkörper nur die Einheiten ± 1 enthält, also $N_k(\mathsf{E}) = \pm 1$ sein muß, so kann A stets von der Form angenommen werden:

$$\mathsf{A} = \mathsf{H}\alpha \quad \text{oder} \quad \mathsf{A} = \mathsf{H} \cdot \xi\sqrt{\mu},$$

wo α eine ganze, ξ eine ganze oder gebrochene Zahl aus $k(\sqrt{m})$ und H eine Einheit des Relativkörpers bezeichnet.

Hieraus würde sich aber ergeben:

$$\mathsf{E} = \frac{\mathsf{A}}{S(\mathsf{A})} = \frac{\mathsf{H}}{S(\mathsf{H})} = \pm \mathsf{H}^2,$$

E wäre also überhaupt keine Grundeinheit. Die Annahme des Beweises ist mithin nicht zulässig. Daher bleibt nur die Möglichkeit übrig, daß $N_k(\mathsf{E}) = -1$ ist.

[Anmerkung. Um Mißverständnisse zu vermeiden, weise ich nochmals darauf hin, daß die Grundkörper $k(\sqrt{-1})$ und $k(\sqrt{-3})$ von der Untersuchung ausgeschlossen sind. Bei beiden sieht man leicht durch eine gesonderte Betrachtung, wie der vorstehende Satz zu modifizieren ist.]

Aus dem soeben bewiesenen Satz kann man jetzt weiter den Schluß ziehen, daß die Klassenanzahl H eines solchen Körpers $K(\sqrt{\mu})$ ungerade ist. (Vergl. hierzu die analoge Betrachtung von Nr. 23, S. 110.)

Angenommen nämlich, die Klassenanzahl des Körpers $K(\sqrt{\mu})$ sei gerade, so gibt es ein Nichthauptideal $\mathfrak{J}$ von der Beschaffenheit, daß $\mathfrak{J}^2 \sim 1$ ist. Dann ist aber auch $S(\mathfrak{J})^2 \sim 1$ und $(\mathfrak{J}S(\mathfrak{J}))^2 \sim 1$. Da andererseits $\mathfrak{J}S(\mathfrak{J}) = \mathfrak{j}$ ein Ideal des Grundkörpers ist und $\mathfrak{j}^h \sim 1$ ausfällt, so muß wegen der Voraussetzung, über h, das eine ungerade ganze Zahl ist, auch $\mathfrak{J}S(\mathfrak{J}) \sim 1$ sein. Aus $\mathfrak{J}^2 \sim 1$ und $\mathfrak{J}S(\mathfrak{J}) \sim 1$ folgt daher $\mathfrak{J} \sim S(\mathfrak{J})$ oder $\mathfrak{J} = (\mathsf{B})S(\mathfrak{J})$, wo B eine gebrochene oder ganze Zahl des Körpers vorstellt, deren Relativnorm alsdann ± 1 sein muß, weil der Körper k nur die Einheiten ± 1 enthält. Ist $N_k(\mathsf{B}) = +1$, so kann man ohne weiteres eine Gleichung $\mathsf{B} = \frac{S(\mathsf{A})}{\mathsf{A}}$ ansetzen, wo A und $S(\mathsf{A})$ ganze Zahlen des Körpers sind; ist aber $N_k(\mathsf{A}) = -1$, so ist $N_k(\mathsf{EB}) = +1$, und man darf wieder $\mathsf{EB} = \frac{S(\mathsf{A})}{\mathsf{A}}$ setzen. In beiden Fällen kann somit die Idealgleichung $\mathfrak{J} = (\mathsf{B})S(\mathfrak{J})$ ersetzt werden durch die andere $(\mathsf{A})\mathfrak{J} = S(\mathsf{A}\mathfrak{J})$. Es würde also wieder jeder in $(\mathsf{A})\mathfrak{J}$ aufgehende ideale Primfaktor auch in $S(\mathsf{A}\mathfrak{J})$ aufgehen müssen.

Weil aber in $K(\sqrt{\mu})$ nur ein einziges ambiges Ideal $\mathfrak{P}$ existiert und man stets ein Ideal $\mathfrak{m}$ des Grundkörpers k angeben kann, so daß $\mathfrak{m} \cdot \mathfrak{P} = \left(\frac{\beta\sqrt{\mu}}{\gamma}\right)$ wird, so ist entweder: $(\mathsf{A})\mathfrak{J} = \mathfrak{j}$, oder: $\mathfrak{m}(\mathsf{A})\mathfrak{J} = \mathfrak{j}\left(\frac{\beta\sqrt{\mu}}{\gamma}\right)$, wo $\mathfrak{j}$ jedesmal ein Ideal aus k bezeichnet. Es wäre daher in beiden Fällen $\mathfrak{J}$ äquivalent einem Ideal des Grundkörpers, ev. einem Hauptideal, und da alsdann $\mathfrak{J}^h \sim \mathfrak{j}^h \sim 1$ neben $\mathfrak{J}^2 \sim 1$ bestünde, so wäre $\mathfrak{J} \sim 1$, was der Voraussetzung über $\mathfrak{J}$ widerspricht.

Zur bequemeren Formulierung der weiteren Sätze hat Herr Hilbert in seinen Abhandlungen über den relativ quadratischen und relativ Abelschen Zahlkörper folgende Bezeichnungen gebraucht[1]):

Definition. Ein zu 2 primes Primideal $\mathfrak{p}$ des Grundkörpers $k(\sqrt{m})$, nach welchem *jede* Einheit in $k(\sqrt{m})$ quadratischer Rest ist, heißt ein *primäres* Primideal, jedes Primideal dagegen, welches nicht dieser Bedingung genügt, heißt ein nicht primäres Ideal.

Da übrigens nach den Voraussetzungen über den Grundkörper die einzigen Einheiten desselben ± 1 sind, so ist jedes zu 2 prime

1) Der Name und der Begriff der primären Zahl ist von C. F. Gauß eingeführt worden. Werke Bd. II. Theoria resid. biquadrat. Com. sec. Nr. 36.

Primideal $\mathfrak{p}$ primär, nach welchem -1 quadratischer Rest ist. Für solche primäre Primideale gilt nun der folgende Satz:

Satz. *Ist $\mathfrak{p}$ ein primäres Primideal des Körpers k, dann gibt es stets eine Zahl π in diesem Körper von der Eigenschaft, daß $(\pi) = \mathfrak{p}^h$ ist und daß die Kongruenz:*

$$\pi \equiv \alpha^2, \ (4)$$

durch eine ganze Zahl α aus k erfüllt werden kann.

Beweis. Der Beweis dieses Satzes gestaltet sich bei den beschränkten oben getroffenen Voraussetzungen sehr einfach.

Entweder ist $\mathfrak{p}$ ein Primideal ersten Grades oder zweiten Grades. Im letztern Fall hat man eben $\mathfrak{p} = (p)$, und da $\mathfrak{p}$ und p prim sind zu 2, so gilt sicher eine der Kongruenzen

$$p \equiv 1, \ (4) \quad \text{oder} \quad -p \equiv 1, \ (4),$$

womit für diesen Spezialfall der Beweis des Satzes erledigt ist.

Ist dagegen $\mathfrak{p}$ ein Primideal ersten Grades, so wird $(p) = \mathfrak{p} \cdot \mathfrak{p}'$ resp. $n(\mathfrak{p}) = p$ und p ist prim zu 2. Nach Nr. 18, S. 82, gilt nun aber für irgend eine zu $\mathfrak{p}$ prime ganze Zahl ϱ des Körpers $k(\sqrt{m})$ stets eine Kongruenz

$$\varrho^{n(\mathfrak{p})-1} \equiv 1, \ (\mathfrak{p}).$$

Damit die Kongruenz $-1 \equiv \xi^2, \ (\mathfrak{p})$ durch eine ganze Zahl ξ des Körpers $k(\sqrt{m})$ befriedigt wird, ist daher notwendig, daß $\frac{n(\mathfrak{p})-1}{2} \equiv 0$, (2), d. h. $p \equiv 1, \ (4)$ ausfällt.

Nun sei etwa

$$\mathfrak{p}^h = (a + b\omega),$$

wo, wie üblich, $\omega = \frac{1+\sqrt{m}}{2}$ ist, dann wird:

$$\begin{aligned}(p^h) &= (a + b\omega)(a + b\omega') \\ &= \left(a^2 + ab + b^2 \frac{1-m}{4}\right).\end{aligned}$$

Weil hierin p eine rationale Primzahl von der Form $p \equiv 1, \ (4)$ ist, so können a und b sicher nicht zugleich gerade Zahlen sein, und da weiter $a^2 + ab + b^2 \frac{1-m}{4} = \left(a + \frac{b}{2}\right)^2 - \frac{m}{4} b^2$ stets positiv ist, bleiben für a und b nur die folgenden Möglichkeiten:

1.) Falls $\frac{1-m}{4} \equiv 1, \ (4)$ ist, muß $a \equiv \pm 1$ und $b \equiv 0$, oder $a \equiv \pm 1$ und resp. $b \equiv \mp 1, \ (4)$ sein.

2.) Falls $\frac{1-m}{4} \equiv 2, \ (4)$ ist, muß $a \equiv \pm 1$, $b \equiv 0, \ (4)$ sein.

3.) Falls $\frac{1-m}{4} \equiv 3$, (4) ist, muß $a \equiv \pm 1$, $b \equiv 0$, oder $a \equiv \pm 1$ und resp. $b \equiv \pm 1$, oder $a \equiv 2$, $b \equiv \pm 1$, (4) sein.

4.) Falls $\frac{1-m}{4} \equiv 0$, (4) ist, muß $a \equiv \pm 1$, $b \equiv 0$, (4) sein.

Unter Berücksichtigung dieser Möglichkeiten läßt sich jetzt durch eine spezielle Diskussion zeigen, daß in der Tat stets eine der beiden Kongruenzen:

$$a + b\omega \equiv (x + y\omega)^2, \ (4)$$

oder

$$-a - b\omega \equiv (x + y\omega)^2, \ (4)$$

durch ganze rationale Zahlen x, y befriedigt werden kann. Anders ausgesprochen ist entweder das System:

$$a - x^2 + \frac{1-m}{4} y^2 \equiv 0, \ (4)$$

$$b - 2xy - y^2 \equiv 0, \ (4)$$

oder das System:

$$-a - x^2 + \frac{1-m}{4} y^2 \equiv 0, \ (4)$$

$$-b - 2xy - y^2 \equiv 0, \ (4)$$

in ganzen rationalen Zahlen x, y lösbar.

Damit ist aber der Satz bewiesen; es ist stets

$$\pi = \pm (a + b\omega) \equiv \alpha^2, \ (4).$$

Von dem eben bewiesenen Satz gilt auch die Umkehrung, wie jetzt gezeigt werden soll.

Satz. *Es sei π eine ganze Zahl des Körpers k, für welche die Kongruenz $\pi \equiv \alpha^2$, (4) durch eine ganze Zahl α desselben Körpers befriedigt werden kann, und es sei ferner (π) die h^{te} Potenz eines zu (2) primen Primideals $\mathfrak{p}$, also $(\pi) = \mathfrak{p}^h$, so ist $\mathfrak{p}$ ein primäres Ideal, d. h. es ist -1 quadratischer Rest nach $\mathfrak{p}$.*

Beweis. Wegen der Voraussetzungen über π enthält die Relativdiskriminante des Körpers $K(\sqrt{\pi})$ nur den einen Primfaktor $\mathfrak{p}$. Dann ist aber die Relativnorm der Grundeinheit E des Körpers $K(\sqrt{\mu})$ gleich -1. Setzen wir etwa $\mathsf{E} = \frac{\sigma + \varrho\sqrt{\pi}}{2\tau}$ (mit Rücksicht auf die Form der ganzen Zahlen des Körpers $K(\sqrt{\pi})$), so ist $\frac{2\sigma}{2\tau}$ eine ganze Zahl, und τ ist höchstens durch $\mathfrak{p}^{\frac{h-1}{2}}$ teilbar. Aus der Kongruenz:

$$-1 = \frac{\sigma^2 - \varrho^2\pi}{4\tau^2}$$

folgt daher

$$-4 \equiv \lambda^2, \left(\frac{\varrho^2\pi}{\mathfrak{r}^2}\right)$$

und umsomehr

$$-4 \equiv \lambda^2, (\mathfrak{p}).$$

Da 2 prim ist zu $\mathfrak{p}$, so gibt es eine ganze Zahl ξ in k von der Beschaffenheit, daß $2\xi \equiv \pm 1, (\mathfrak{p})$ oder $4\xi^2 \equiv 1, (\mathfrak{p})$ gesetzt werden kann, und damit erhält man schließlich:

$$-1 \equiv \alpha^2, (\mathfrak{p}),$$

w. z. b. w.

Die zwei soeben bewiesenen Sätze berechtigen nun zu der folgenden Definition:

Definition. Wenn $\mathfrak{p}$ ein primäres Primideal des Körpers k ist und die ganze Zahl π in der Gleichung $(\pi) = \mathfrak{p}^h$ so gewählt wird, daß $\pi \equiv \alpha^2, (4)$ ausfällt, so heißt π eine *primäre* Zahl des primären Primideals $\mathfrak{p}$.

Satz. *Wenn $\mathfrak{p}$ ein primäres Primideal des Körpers k, und π eine Primärzahl von $\mathfrak{p}$ ist, wenn ferner $\mathfrak{r}$ irgend ein anderes Primideal aus k bezeichnet und $(\varrho) = \mathfrak{r}^h$ gesetzt wird, so folgt aus $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ auch $\left(\frac{\varrho}{\mathfrak{p}}\right) = +1$.*

$\left(\frac{\pi}{\mathfrak{r}}\right)$ bezeichnet hier wieder das auf Ideale ausgedehnte Legendresche Symbol.

Beweis. Wegen der Voraussetzung $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ zerfällt das Primideal $\mathfrak{r}$ in dem Relativkörper $K(\sqrt{\pi})$ in ein Produkt aus zwei relativ konjugierten Idealen:

$$\mathfrak{r} = (\mathfrak{r}, \mathsf{A})(\mathfrak{r}, S(\mathsf{A})).$$

Weil ferner π eine Primärzahl von $\mathfrak{p}$ ist, so enthält also die Relativdiskriminante von $K(\sqrt{\pi})$ nur den einen Primfaktor $\mathfrak{p}$, und es gibt eine ungerade rationale Zahl u von der Eigenschaft, daß:

$$\mathfrak{r}^u = (\mathsf{P}) \cdot (S(\mathsf{P}))$$

ausfällt, wo P und $S(\mathsf{P})$ ganze Zahlen des Relativkörpers $K(\sqrt{\pi})$ bedeuten. Erhebt man beide Seiten dieser Gleichung zur Potenz h, so kann man schreiben:

$$(\varrho)^u = (\mathsf{P}_1)(S(\mathsf{P}_1)),$$

oder es ist:

$$\varrho^u \doteq \frac{\alpha + \beta\sqrt{\pi}}{2\gamma} \cdot \frac{\alpha - \beta\sqrt{\pi}}{2\gamma}.$$

Nach den Eigenschaften der ganzen Zahlen des Relativkörpers sind $\frac{\alpha}{\gamma}$ und $\frac{\beta\sqrt{\pi}}{\gamma}$ ganze Zahlen desselben, und es ist mithin:

$$4\varrho^u \equiv \nu^2,\ (\mathfrak{p}).$$

Bestimmt man jetzt noch ξ so, daß

$$2\varrho^{\frac{u-1}{2}}\xi \equiv 1,\ (\mathfrak{p})$$

wird, so ist:

$$4\xi^2\varrho^u \equiv \varrho \equiv \xi^2\nu^2,\ (\mathfrak{p})$$

oder schließlich:

$$\varrho \equiv \alpha^2,\ (\mathfrak{p}),$$

also $\left(\frac{\varrho}{\mathfrak{p}}\right) = +1$, wie der Satz behauptet.

Durch eine wiederholte Anwendung dieses Satzes beweist man den weiteren Satz:

Satz. *Wenn* $\mathfrak{p}$ *und* $\mathfrak{p}_1$ *zwei primäre Primideale sind und* π *resp.* π_1 *zugehörige Primärzahlen, so gilt stets die Gleichung:*

$$\left(\frac{\pi}{\mathfrak{p}_1}\right) = \left(\frac{\pi_1}{\mathfrak{p}}\right).$$

Beweis. Aus $\left(\frac{\pi}{\mathfrak{p}_1}\right) = +1$ folgt nach dem vorhergehenden Satz sofort $\left(\frac{\pi_1}{\mathfrak{p}}\right) = +1$. Wenn nun $\left(\frac{\pi}{\mathfrak{p}_1}\right) = -1$ ist, so muß ebenso $\left(\frac{\pi_1}{\mathfrak{p}}\right) = -1$ sein. Wäre nämlich $\left(\frac{\pi_1}{\mathfrak{p}}\right) = +1$, so folgte aus dem vorhergehenden Satze $\left(\frac{\pi}{\mathfrak{p}_1}\right) = +1$ im Widerspruch zu der an zweiter Stelle gemachten Annahme.

Wir haben hiermit wichtige, aber doch nur kleine Teile (Ergänzungssätze) des allgemeinen Reziprozitätsgesetzes bewiesen. Bezüglich dieses allgemeinen Gesetzes verweise ich den Leser auf die Abhandlungen der Herren Hilbert und Furtwängler. Nur um nochmals die Bedeutung des von Herrn Hilbert eingeführten Symbols des *Normenrestes* und *Normennichtrestes* zu belegen, möge angeführt werden, daß die Formulierung des Gesetzes sehr einfach wird mit Benützung dieses Symbols in seiner Erweiterung auf allgemeine Grundkörper. Ganz analog, wie bei dem quadratischen Zahlkörper, läßt sich durch das Symbol des Normenrestes eine Einteilung der Idealklassen des relativquadratischen Körpers in Geschlechter begründen. Der Existenzbeweis für gewisse aus den überhaupt denkbaren Geschlechtern liefert dann eben das Reziprozitätsgesetz.[1]

---

1) Vergl. D. Hilbert, Math. Ann. Bd. 51, S. 85. Das allgemeine quadra-

In den oben behandelten Fällen beruhte die Möglichkeit für einen einfachen Beweis auf dem Umstand, daß die Klassenanzahl des Relativkörpers ungerade ist, wonach dann sämtliche Klassen desselben zum selben Geschlecht gehören.

55. Beispiele für Klassenkörper.

Zum Schluß mögen noch die Eigenschaften der Relativkörper in einigen bisher ausgeschiedenen Fällen erwähnt werden: erstens, wenn der Grundkörper imaginär ist und eine gerade Klassenanzahl besitzt, und zweitens, wenn der Grundkörper reell ist.

1. Beispiel. Grundkörper sei der Körper $k(\sqrt{-5})$, für welchen ± 1 die einzigen Einheiten sind. Die Zahlen 1, $\omega = \sqrt{-5}$ bilden eine Basis des Körpers, dessen Klassenanzahl $h = 2$ ist.

Die interessanteste Frage, die zunächst zu beantworten ist, ist die folgende: Gibt es relativ quadratische Körper, deren Relativdiskriminante in bezug auf k gleich ± 1 wird? Ein solcher Relativkörper enthält offenbar keine ambigen Ideale und wird als ein *unverzweigter* Oberkörper bezeichnet.

Da nun die dem Körper $k(\sqrt{-5})$ angehörige Zahl $\mu = -1$ überhaupt keinen Primfaktor enthält, und die Kongruenz

$$-1 \quad \alpha^2, \ (4)$$

für $\alpha = \sqrt{-5}$ erfüllt ist, so ist die Relativdiskriminante von $K(\sqrt{-1})$ prim zu (2) und enthält also überhaupt keinen Primfaktor, d. h. $K(\sqrt{-1})$ ist ein Körper der verlangten Art.

Nach Herrn Hilbert heißt ein relativ quadratischer Körper $K(\sqrt{\mu})$, der in bezug auf einen Unterkörper mit der Klassenanzahl 2 die Relativdiskriminante ± 1 besitzt, Klassenkörper dieses Unterkörpers.[1]

tische Reziprozitätsgesetz, S. 108. Das allgemeine quadratische Reziprozitätsgesetz für einen quadratischen Grundkörper von der Klassenanzahl 1 hat Herr Dörrie in seiner schon früher zitierten Dissertation bewiesen. Zahlenmaterial findet sich bei G. Rückle, „Quadratische Reziprozitätsgesetze im algebr. Zahlkörper", Diss. Göttingen 1901.

1) Die allgemeinen Begriffe und Sätze, welche in dieser Nummer an einigen Zahlenbeispielen erläutert sind, schließen sich an entsprechende Begriffe in der Theorie der komplexen Multiplikation der elliptischen Funktionen an. Die ersten Ansätze dieser Entwicklungen, insbesondere der Ausdruck Klassenkörper, rühren von L. Kronecker her. Wegen der weiteren Ausführung und für die Beweise verweise ich auf: D. Hilbert, Nachr. von der kgl. Ges. d. Wissensch. zu

In unserem Beispiel ist also $K(\sqrt{-1})$ ein *Klassenkörper des quadratischen Grundkörpers* $k(\sqrt{-5})$.

Wählt man als eine Basis dieses Klassenkörpers die vier Zahlen:

$$1, \quad \omega = \sqrt{-5}, \quad \Omega = \frac{\sqrt{-5}+\sqrt{-1}}{2}, \quad \Omega_1 = \sqrt{-5}\,\frac{\sqrt{-5}+\sqrt{-1}}{2},$$

so ist Ω zugleich eine Einheit von der Beschaffenheit, daß:

$$\Omega S(\Omega) = \frac{-5+1}{4} = -1,$$

wird, und es ergeben sich bei der Untersuchung der Zerlegung der Zahlen und Ideale des Grundkörpers die in den folgenden Sätzen formulierten Tatsachen. Jeder der Sätze spricht eine auch ganz allgemein gültige charakteristische Eigenschaft des Klassenkörpers aus.

1.) Eine Primzahl p, welche im Körper $k(\sqrt{-5})$ unzerlegbar ist, muß im Relativkörper $K(\sqrt{-1})$ in das Produkt zweier Primideale zerfallen. Denn wenn $\left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right) = -1$ ist, so ist entweder $\left(\frac{5}{p}\right) = +1$ oder $\left(\frac{-1}{p}\right) = +1$. Daraus folgt aber, daß die Zahl p im Körper $k(\sqrt{+5})$ oder $k(\sqrt{-1})$ zerfällt, und weil die sämtlichen Zahlen dieser beiden Körper dem Relativkörper $K(\sqrt{-1})$ angehören, zerfällt also p in diesem letzteren.

So ist beispielsweise $(p) = (11)$ ein Primideal zweiten Grades im Körper $k(\sqrt{-5})$, es ist aber $\left(\frac{5}{11}\right) = 1$ und entsprechend:

$$(11) = (4+\sqrt{5})(4-\sqrt{5}) = (9+2\Omega_1)(1-2\Omega_1).$$

Ganz ebenso sind die Primzahlen $p = 13,\ 17,\ 19,\ 31$ im Körper $k(\sqrt{-5})$ unzerlegbar, dagegen wird im Relativkörper:

$$\begin{aligned}
(13) &= (3+2\sqrt{-1})(3-2\sqrt{-1}) = (3-2\omega+4\Omega)(3+2\omega-4\Omega),\\
(17) &= (4+\sqrt{-1})(4-\sqrt{-1}) \quad = (4-\omega+2\Omega)(4+\omega-2\Omega),\\
(19) &= \left(4+\frac{1+\sqrt{5}}{2}\right)\left(4+\frac{1-\sqrt{5}}{2}\right) = (7+\Omega_1)(2-\Omega_1),\\
(31) &= (6+\sqrt{5})(6-\sqrt{5}) \quad = (11+2\Omega_1)(1-2\Omega_1).
\end{aligned}$$

Göttingen, math.-phys. Klasse, 1898, S. 370 ff., sowie Acta math. Bd. 26, 1902, S. 99 ff. Diese Abhandlung ist eine Ergänzung derjenigen aus Math. Ann. Bd. 51 über relativ quadr. Körper. Vergl. ferner die Dissert. von R. Fueter, „Der Klassenkörper der quadratischen Körper und die komplexe Multiplikation", Göttingen 1903, Kap. I, II.

2.) Ist p eine Primzahl, welche im Grundkörper $k(\sqrt{-5})$ zerlegbar ist in das Produkt $\mathfrak{p}\cdot\mathfrak{p}'$, so hat man zwei Fälle zu unterscheiden:

Entweder es ist 2a.) $p \equiv 1,\ (4)$, oder es ist 2b.) $p \equiv 3,\ (4)$.

2a.) Im ersten Fall ist die Kongruenz

$$-1 \equiv \alpha^2,\ (\mathfrak{p})$$

stets durch eine ganze Zahl α des Grundkörpers lösbar. In der Tat, da $n(\mathfrak{p}) = p$ wird, so ist jede ganze Zahl aus k einer der ganzen rationalen Zahlen zwischen 1 und p modulo $(\mathfrak{p})$ kongruent; weil nun aber die Kongruenz

$$-1 \equiv x^2,\ (p)$$

lösbar ist, ist umsomehr auch die Kongruenz

$$-1 \equiv \alpha^2,\ (\mathfrak{p})$$

lösbar und ebenso die Kongruenz

$$-1 \equiv \alpha_1^2,\ (\mathfrak{p}').$$

Die Ideale $\mathfrak{p}$ und $\mathfrak{p}'$ sind darum im Relativkörper $K(\sqrt{-1})$ weiter *zerlegbar*. Die Ideale $\mathfrak{p}$, $\mathfrak{p}'$ sind aber *Hauptideale*, wie die folgende Überlegung zeigt: Der Grundkörper $k(\sqrt{-5})$ hat die Diskriminante -20, welche die beiden Primzahlen 2 und 5 als Faktoren enthält. Die zwei Klassen (Hauptklasse und Nichthauptklasse) des Körpers gehören danach zu *zwei verschiedenen* Geschlechtern, und man sieht sofort ein, daß $\mathfrak{p}$, $\mathfrak{p}'$ zum Hauptgeschlecht und folglich zur Klasse der Hauptideale gehören. In der Tat ist wegen: $p \equiv 1,\ (4)$ auch $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{\pm 5}{p}\right) = 1$.

2b.) Anders verhält sich der zweite Fall. Hier kann die Kongruenz:

$$-1 \equiv \alpha^2,\ (\mathfrak{p})$$

keine Lösung besitzen. Denn weil wieder α kongruent einer ganzen rationalen Zahl mod $(\mathfrak{p})$ sein muß, so müßte auch die Kongruenz

$$-1 \equiv x^2,\ (p)$$

durch eine ganze rationale Zahl x lösbar sein, was bekanntlich nicht zutrifft.

Die Primideale $\mathfrak{p}$ der zweiten Klasse, d. h. der Klasse der Nichthauptideale, bleiben somit auch im Relativkörper $K(\sqrt{-1})$ Primideale. Diese Primideale sind aber Hauptideale des Oberkörpers $K(\sqrt{-1})$, wie die folgende kleine Überlegung zeigt.

Die Zahl 2 zerfällt im Körper $k\sqrt{-1}$, indem

$$2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$$

ist. Setzt man $\mathfrak{z} = (2,\ 1 + \sqrt{-5})$ und bezeichnet $\mathfrak{p}$ *irgend* ein Primideal der zweiten Klasse des Körpers $k(\sqrt{-5})$, so wird $\mathfrak{z}\mathfrak{p} = (\alpha)$, wo α eine ganze Zahl des Grundkörpers ist. Also ist $\mathfrak{z}^2\mathfrak{p}^2 = (\alpha)^2$, und indem man $\mathfrak{p}^2 = (\pi)$ schreibt, folgt $\pm 2\pi = \alpha^2$ oder $\pm 4\pi = \alpha^2 \cdot 2$. Im Relativkörper ist daher

$$(\pi) = \left(\frac{\alpha(1+\sqrt{-1})}{2}\right)\left(\frac{\alpha(1-\sqrt{-1})}{2}\right).$$

Da offenbar jede der beiden Zahlen $\frac{\alpha(1+\sqrt{-1})}{2}$ und $\frac{\alpha(1-\sqrt{-1})}{2}$ eine ganze Zahl in $K(\sqrt{-1})$ ist (denn ihre Summe und ihr Produkt sind ja ganz), so ist $\mathfrak{p}^2$ im Körper $K(\sqrt{-1})$ gleich dem Produkt zweier relativ konjugierter Hauptideale. Weil ferner $\mathfrak{p}$ im Relativkörper nicht zerfällt und die beiden Zahlen $\frac{\alpha(1+\sqrt{-1})}{2}$ und $\frac{\alpha(1-\sqrt{-1})}{2}$ sich nur um einen Einheitsfaktor $\sqrt{-1}$ unterscheiden, so gilt im Relativkörper die Gleichung $\mathfrak{p} = \left(\frac{\alpha(1+\sqrt{-1})}{2}\right)$. D. h. jedes Primideal ersten Grades des Körpers $k(\sqrt{-5})$, das in diesem Körper Nichthauptideal ist, wird im Relativkörper zum Hauptideal.

Die Resultate von 1.) und 2.) ergeben zusammen den folgenden Satz:

Satz. *Diejenigen Primideale des Grundkörpers $k(\sqrt{-5})$, welche Hauptideale sind, zerfallen im Klassenkörper in ein Produkt zweier Ideale; die Primideale dagegen, welche in $k(\sqrt{-5})$ Nichthauptideale sind, bleiben auch im Klassenkörper Primideale, sie werden aber zu Hauptidealen.*

Verschiedene Zahlenbeispiele mögen diesen Satz weiter erläutern. Es ist:

$$\begin{aligned}
(5) &= (\sqrt{-5})^2,\\
(29) &= (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}),\\
(41) &= (6 + \sqrt{-5})(6 - \sqrt{-5}),\\
(61) &= (4 + 3\sqrt{-5})(4 - 3\sqrt{-5}),
\end{aligned}$$

also sind $(\sqrt{-5})$, $(3 + 2\sqrt{-5})$, $(3 - 2\sqrt{-5})$ usw. usw. Hauptprimideale des Körpers $k(\sqrt{-5})$, welche im Klassenkörper zerfallen. Man findet leicht:

$$(\sqrt{-5}) = (1+\Omega)(1+S(\Omega)),$$
$$(3+2\sqrt{-5}) = (1-\sqrt{-5}+\sqrt{-1})(1-\sqrt{-5}-\sqrt{-1}),$$
$$(3-2\sqrt{-5}) = (1+\sqrt{-5}+\sqrt{-1})(1+\sqrt{-5}-\sqrt{-1}),$$
$$(6+\sqrt{-5})$$
$$= \left(\frac{5+\sqrt{-5}-(3-\sqrt{-5})\sqrt{-1}}{2}\right)\left(\frac{5+\sqrt{-5}+(3-\sqrt{-5})\sqrt{-1}}{2}\right)$$
$$= (5+2\sqrt{-5}-3\Omega+\Omega_1)(5+2\sqrt{-5}-S(\Omega)+S(\Omega_1));$$

eine ganz analoge Zerlegung ergibt sich für $(6-\sqrt{-5})$ durch Vertauschung von $+\sqrt{-5}$ und $-\sqrt{-5}$; ferner ist:

$$(4+3\sqrt{-5})$$
$$= \left(\frac{5+\sqrt{-5}+(1+\sqrt{-5})\sqrt{-1}}{2}\right)\left(\frac{5+\sqrt{-5}-(1+\sqrt{-5})\sqrt{-1}}{2}\right)$$
$$= (5+\Omega+\Omega_1)(5+\Omega+S(\Omega_1))$$

nebst einer ähnlichen Zerlegung für $(4-3\sqrt{-5})$.

Das Verhalten der Nichthauptideale des Grundkörpers im Klassenkörper illustrieren die folgenden Beispiele. Es ist

$$(2, 1+\sqrt{-5}) = (2, 1+\sqrt{-5}, (1+\sqrt{-1})^2, 1+\sqrt{-1}) = (1+\sqrt{-1}),$$

indem:

$$(2) = (1+\sqrt{-1})(1-\sqrt{-1}),$$
$$(1+\sqrt{-5}) = (1+\sqrt{-1})(-2+S(\Omega)-\Omega_1) \text{ ist;}$$

analog ist:

$$(3,\ 1+\sqrt{-5}) = (-2+S(\Omega)-\Omega_1),$$
$$(3,\ 1-\sqrt{-5}) = (3-\Omega+\Omega_1),$$

und ebenso:

$$(7,\ 3+\sqrt{-5}) = (4+2\omega-3S(\Omega)+\Omega_1),$$

ferner:

$$(23,\ 8+\sqrt{-5}) = (8+\omega+\Omega+3\Omega_1) \text{ usw.}$$

Durch wiederholte Anwendung des eben erläuterten Satzes folgt auch die Richtigkeit für die Fälle, wo das Wort Primideal jedesmal durch Ideal ersetzt werden kann.

Schließlich läßt sich für das Beispiel des Körpers $k(\sqrt{-5})$ noch zeigen, *daß der Klassenkörper eine ungerade Klassenanzahl besitzt.*

Angenommen $\mathfrak{J}$ sei ein Nichthauptideal des Körpers $K(\sqrt{-1})$ von der Art, daß $\mathfrak{J}^2 \sim 1$ ausfällt. Da nun jedesmal $\mathfrak{J}S(\mathfrak{J})$ ein Ideal

des Grundkörpers vorstellt und somit, wie eben gezeigt wurde, ein Hauptideal desselben oder des Klassenkörpers ist, so würde:

$$\mathfrak{J}^2 \sim \mathfrak{J} S(\mathfrak{J}),$$

oder:

$$\mathfrak{J} \sim S(\mathfrak{J})$$

sein.

Setzt man alsdann $\mathsf{B} = \frac{\mathfrak{J}}{S(\mathfrak{J})}$, dann wird $N_k(\mathsf{B}) = \pm 1$. Falls $N_k(\mathsf{B}) = +1$ ist, kann $\mathsf{B} = \frac{S(\mathsf{A})}{\mathsf{A}}$, und falls $N_k(\mathsf{B}) = -1$ ist, wegen $N_k(\mathsf{E}) = -1$, analog $\mathsf{EB} = \frac{S(\mathsf{A})}{\mathsf{A}}$ angenommen werden, wo A jetzt eine ganze Zahl des Klassenkörpers bedeutet. In beiden Fällen ergibt sich sodann:

$$(\mathsf{A})\mathfrak{J} = S(\mathsf{A}\mathfrak{J}),$$

es wäre somit $(\mathsf{A})\mathfrak{J}$ ein Ideal des Grundkörpers oder das Produkt eines ambigen Ideals des Klassenkörpers mit einem Ideal des Grundkörpers. Weil aber die Relativdiskriminante des Klassenkörpers überhaupt kein Primideal und der Klassenkörper kein ambiges Ideal enthält, so ist $(\mathsf{A}\mathfrak{J})$ ein Ideal des Grundkörpers und daher $\mathfrak{J} \sim 1$; d. h. wenn das Quadrat eines Ideals $\mathfrak{J}$ ein Hauptideal ist, so ist auch $\mathfrak{J}$ selbst schon Hauptideal.

Nimmt man nun die Klassenanzahl des Relativkörpers $H = 2^a u$ an, wo u eine ungerade ganze Zahl ist, so würde für jedes Ideal der Reihe nach sich ergeben:

$$\mathfrak{J}^{2^a u} \sim 1, \quad \mathfrak{J}^{2^{a-1} u} \sim 1, \ldots \quad \mathfrak{J}^u \sim 1.$$

Die Annahme des Beweises ist damit widerlegt, die Klassenanzahl ist ungerade.

Man übersieht unmittelbar, daß die soeben für den Körper $k(\sqrt{-5})$ angestellten Betrachtungen fast wörtlich übertragbar sind auf jeden Grundkörper $k(\sqrt{m})$ mit der Klassenanzahl 2, der durch eine negative Primzahl m von der Form $m \equiv 3, (4)$ bestimmt ist. Als ein Klassenkörper für jeden solchen Grundkörper kann der Relativkörper $K(\sqrt{-1})$ gewählt werden; die Grundeinheit ε_1 des Körpers $k(\sqrt{-m}) = k(\sqrt{-1}\sqrt{m})$, für welche bekanntlich $n(\varepsilon_1) = -1$ wird, ist zugleich eine Einheit in $K(\sqrt{-1})$ mit einer Relativnorm gleich -1.

Indessen gelten die Sätze, welche wir eben im Beispiel kennen gelernt haben, überhaupt für jeden Grundkörper mit der Klassenanzahl 2, wie Herr Hilbert bewiesen hat.

Beschränken wir uns vorläufig noch weiter auf imaginäre quadratische Grundkörper $k(\sqrt{m})$, so kann man wegen der Bedingung $h=2$ zunächst aussagen, daß das Geschlecht dieser Grundkörper $g \leqq 2$ sein muß. Es ist aber bekanntlich $g = 2^{r-1}$, wenn r die Anzahl der voneinander verschiedenen in der Diskriminante des Körpers $k(\sqrt{m})$ aufgehenden Primzahlen angibt. Falls die Zahl m die Kongruenz: $m \equiv 1,\ (4)$ befriedigt und nur eine rationale Primzahl enthält, wird $r=1$ und $g=1$, und die Klassenanzahl von $k(\sqrt{m})$ ist ungerade. Für $h=2$ bleibt als einzige Möglichkeit nur $g=2$ und $r=2$ übrig, d. h. es ist entweder m eine negative Primzahl von der Form $m \equiv 3,\ (4)$; dann haben wir den schon behandelten Fall, oder es ist $m \equiv 2,\ (4)$ oder $m \equiv 1,\ (4)$; die Zahl m enthält im ersten Fall den Faktor 2 und eine zweite Primzahl von der Form $4n \pm 3$, im zweiten Fall enthält m eine positive rationale Primzahl $p \equiv 1,\ (4)$ und eine zweite positive rationale Primzahl $q \equiv 3,\ (4)$.

Die nächsten Zahlenbeispiele zeigen, daß diese Möglichkeiten auch wirklich auftreten.

2. Beispiel. Der Körper $k(\sqrt{-22})$ hat die Diskriminante $d = -88$, die Klassenanzahl $h=2$ und das Geschlecht $g=2$. Wenn nun $\mathfrak{p}$ irgend ein zu 2 primes Primideal, aber Nichthauptideal, darstellt und $(\pi) = \mathfrak{p}^2$ gesetzt wird, so ist die Kongruenz $\pm\pi \equiv \alpha^2,\ (4)$ stets für eine der beiden Zahlen $+\pi$ oder $-\pi$ durch eine ganze Zahl des Körpers erfüllt.

Denn ist p die durch $\mathfrak{p}$ teilbare rationale Primzahl, und schreibt man ferner $\pi = a + b\sqrt{-22}$, so ist $p^2 = \pi \cdot \pi' = a^2 + 22b^2$. Wegen $p^2 \equiv 1,\ (4)$ muß a ungerade, b gerade sein, daher ist die Kongruenz:

$$\pm\left(a + b\sqrt{-22}\right) \equiv \alpha^2,\ (4)$$

durch eine ganze Zahl α aus $k(\sqrt{-22})$ erfüllbar. Wird $\pi_1 = \pm\pi$ geschrieben für diejenige Zahl, für welche $\pi_1 \equiv \alpha^2,\ (4)$ ausfällt, so stellt auf Grund der allgemeinen Sätze über Relativkörper der Körper $K(\sqrt{\pi_1})$ in bezug auf den Grundkörper $k(\sqrt{-22})$ einen Relativkörper dar, dessen Relativdiskriminante kein von ± 1 verschiedenes Ideal enthält.

Es sei z. B. $\mathfrak{p} = (11, \sqrt{-22})$, so wird $\mathfrak{p}^2 = (11)$, und $K(\sqrt{-11})$ ist alsdann Klassenkörper des Grundkörpers $k(\sqrt{-22})$, indem wieder folgende Sätze gelten:

1. **Satz.** *Die Relativdiskriminante des Relativkörpers* $K(\sqrt{-11})$ *in bezug auf den Körper* $k(\sqrt{-22})$ *ist eine Einheit.*

Die sämtlichen ganzen Zahlen des Relativkörpers lassen sich u. a. durch die vier Zahlen:

$$1, \quad \omega = \sqrt{-22}, \quad \Omega = \frac{11 + \sqrt{-11}}{22}, \quad \Omega_1 = \sqrt{-22}\,\frac{11 + \sqrt{-11}}{22}$$

als Basiszahlen darstellen.

Da der Relativkörper alle Zahlen der quadratischen Körper $k(\sqrt{-11})$ und $k(\sqrt{2})$ enthält, so gilt mit Rücksicht auf die Charakterensysteme der Ideale ferner der Satz:

2. Satz. *Jedes Hauptprimideal des Körpers $k(\sqrt{-22})$ zerfällt im Körper $K(\sqrt{-11})$ in zwei voneinander verschiedene relativ konjugierte Primideale.*

Schließlich ergibt sich für das Verhalten der Nichthauptideale des Körpers $k(\sqrt{-22})$ der Satz:

3. Satz. *Die Primideale des Grundkörpers $k(\sqrt{-22})$, welche nicht der Hauptklasse angehören, bleiben auch im Relativkörper $K(\sqrt{-11})$ Primideale, sie werden aber zu Hauptidealen.*

Man sieht nämlich zunächst, daß das Ideal $(11, \sqrt{-22})$ im Relativkörper zum Hauptideal wird, indem $(11, \sqrt{-22}) = (\sqrt{-11})$ ist. Falls nun $\mathfrak{p}$ ein Nichthauptideal bezeichnet, so ist $(11, \sqrt{-22}) \cdot \mathfrak{p} = (\alpha)$ ein Hauptideal des Grundkörpers, also wird $(11)\mathfrak{p}^2 = \alpha^2$, oder $\mathfrak{p}^2 = \frac{(\alpha)^2 \cdot (\sqrt{-11})^2}{11^2}$.

Nun ist $\frac{\alpha\sqrt{-11}}{11}$ seinerseits eine ganze Zahl des Relativkörpers, und somit $\mathfrak{p}$ ein Hauptideal desselben.

Auf Grund der drei vorausgehenden Sätze ergibt sich dann zuletzt noch die folgende Tatsache:

4. Satz. *Die Klassenanzahl des Relativkörpers $K(\sqrt{-11})$ ist eine ungerade Zahl.*

3. Beispiel eines imaginären Grundkörpers $k(\sqrt{-15})$, bei welchem $-m = 3 \cdot 5$ ist.

Dieser Körper hat die Diskriminante $d = -15$, die Basis $1, \omega = \frac{1 + \sqrt{-15}}{2}$ und die Klassenanzahl und das Geschlecht 2.

Aus der letztern Tatsache folgt, daß alle rationalen Primzahlen, für welche $\left(\frac{-15}{p}\right) = +1$, $\left(\frac{p}{3}\right) = 1$, $\left(\frac{p}{5}\right) = +1$ wird, im Körper $k(\sqrt{-15})$ in das Produkt zweier *Hauptideale* zerfallen.

Es sei $\mathfrak{p}$ irgend ein zu 2 primes Primideal, aber kein Hauptideal und $(\pi) = \mathfrak{p}^2$, so läßt sich wiederum beweisen, daß $\pm \pi \equiv \alpha^2, (4)$ ist. Nimmt man z. B. $\mathfrak{p} = (3, \sqrt{-15})$ oder $\mathfrak{p} = (5, \sqrt{-15})$, so findet sich, daß in bezug auf den Körper $k(\sqrt{-15})$ die Relativkörper $K(\sqrt{-3})$ oder $K(\sqrt{5})$ Klassenkörper mit denselben Eigenschaften sind, welche sich in den früheren Beispielen ergaben.

Diese Beispiele geben einen klaren Einblick in die Eigenschaften der imaginären quadratischen Körper und der quadratischen Relativkörper. Besonders merkwürdig ist die Existenz des Klassenkörpers, als eines Körpers, in dem alle Nichthauptideale des Unterkörpers zu Hauptidealen werden.

Von dem Verhalten der imaginären quadratischen Grundkörper ist das Verhalten der reellen Körper ganz wesentlich verschieden.

Wir erklären zunächst einen von Herrn Hilbert (nach dem Vorgange von Gauß und Dedekind[1]) aufgestellten Begriff, nämlich den Begriff der total positiven und primären Zahl. Für einen reellen quadratischen Körper gilt die folgende Definition:

Definition. Eine Zahl α des reellen quadratischen Körpers $k(\sqrt{m})$ heißt *total positiv*, wenn α und ihre Konjugierte α' positive Größen sind. Wenn ferner α eine ganze zu 2 prime total positive Zahl bedeutet und $\alpha \equiv \nu^2, (4)$ ist, für eine ganze Zahl ν aus $k(\sqrt{m})$, so heißt α eine *primäre Zahl* des Körpers $k(\sqrt{m})$.

Es ist weiter zweckmäßig, an Stelle des bisher ausschließlich verwendeten Äquivalenzbegriffes einen spezielleren (vgl. Nr. 33, S. 173) zu setzen in der nachstehenden Weise:

Definition. Zwei Ideale $\mathfrak{j}$, $\mathfrak{k}$ des Körpers $k(\sqrt{m})$ sollen im engeren Sinne äquivalent heißen, wenn ihr Quotient $\frac{\mathfrak{j}}{\mathfrak{k}} = \alpha$, gleich einer total positiven Zahl des Körpers k ist. Irgend zwei Ideale, die nach *dieser* Definition äquivalent sind, gehören zu derselben Idealklasse.

Die Klassenanzahl im engeren Sinne soll mit dem Buchstaben $\bar{h}$ bezeichnet werden.[1])

In der Gleichung $\frac{\mathfrak{j}}{\mathfrak{k}} = \alpha$ ist ja die Zahl α nur bis auf einen Einheitsfaktor bestimmt. Es kommt daher bei der Bestimmung der

1) Vergl. Dedekind, in Vorles. über Zahlentheorie von Dirichlet-Dedekind, 4. Aufl., Suppl. XI, S. 578.

Klassenanzahl $\bar{h}$ augenscheinlich darauf an, ob die Norm der Grundeinheit des quadratischen Körpers gleich $+1$ oder -1 ist.

In der Tat, sei erstens ε die positive Grundeinheit in $k(\sqrt{m})$ und $n(\varepsilon) = -1$, so ist ε' negativ, und daher ist, falls wir α positiv voraussetzen, jedenfalls eine der beiden Zahlen α oder $\alpha\varepsilon$ total positiv. Wenn nun die Klassenanzahl von k im weiteren Sinne h ist, so bleibt auch $\bar{h} = h$.

Ist zweitens ε die positive Grundeinheit in $k(\sqrt{m})$ und $n(\varepsilon) = +1$, so ist ε' ebenfalls positiv, oder es ist ε total positiv. Der Quotient α, welcher durch die Gleichung $\frac{\mathfrak{j}}{\mathfrak{k}} = \alpha$ definiert ist, ist daher von vornherein total positiv oder nicht. In diesem Falle zerfällt jede Klasse des Körpers in zwei neue Klassen im engeren Sinne.

Denn falls α_1 eine positive Zahl mit negativer Norm bezeichnet, so folgt aus der Äquivalenz zweier Ideale $\mathfrak{j}$ und $\mathfrak{k}$ im weiteren Sinne, stets $\mathfrak{j} \not\sim (\alpha_1)\mathfrak{k}$ im engeren Sinne u. v. v., während bei der weiteren Fassung des Äquivalenzbegriffes $\mathfrak{k}$ und $(\alpha_1)\mathfrak{k}$ äquivalent sind.

Nimmt man die Klassenanzahl von k im weiteren Sinne gleich h an, so ist die Klassenanzahl im engeren Sinne: $\bar{h} = 2h$. U. a. ist für:

$$k(\sqrt{5}):\quad \varepsilon = \omega = \frac{1+\sqrt{5}}{2},\quad n(\varepsilon) = -1;\quad h = 1 \text{ und } \bar{h} = 1,$$

$$k(\sqrt{7}):\quad \varepsilon = 8 + 3\sqrt{7},\quad n(\varepsilon) = +1;\quad h = 1 \text{ und } \bar{h} = 2,$$

$$k(\sqrt{10}):\quad \varepsilon = 3 + \sqrt{10},\quad n(\varepsilon) = -1;\quad h = 2 \text{ und } \bar{h} = 2,$$

$$k(\sqrt{15}):\quad \varepsilon = 4 + \sqrt{15},\quad n(\varepsilon) = +1;\quad h = 2 \text{ und } \bar{h} = 4$$

Es läßt sich nun allgemein beweisen, daß zu einem Körper mit *ungerader* Klassenanzahl $\bar{h}$ überhaupt kein unverzweigter relativ quadratischer Oberkörper existieren kann, daß dagegen unverzweigte Relativkörper für alle andern Körper wirklich vorhanden sind. Für einen Körper mit der Klassenanzahl $\bar{h} = 2$ ist ein solcher Körper zugleich Klassenkörper mit denselben Eigenschaften, wie wir sie früher für Klassenkörper von imaginären Grundkörpern kennen gelernt haben.

Wir betrachten als Beispiel den speziellen Fall $k(\sqrt{+5})$, mit der Klassenanzahl $h = \bar{h} = 1$. Würde für diesen Grundkörper ein unverzweigter relativ quadratischer Oberkörper existieren, und wäre dieser durch die ganze Zahl μ aus k bestimmt, so könnte μ, abgesehen von quadratischen Zahlenfaktoren, eben nur Einheiten und ev. Faktoren von 2 enthalten. Da μ prim zu 2 sein muß, so hat man nur noch zu entscheiden, ob $\mu = -1$ oder $\pm\,\omega$ gesetzt werden darf.

Im letztern Fall ist zu entscheiden, ob die Kongruenz $\pm\omega \equiv \alpha^2$, (4) durch eine ganze Zahl α des Körpers k erfüllbar ist. Setzt man $\alpha = x + y\omega$ und $\alpha^2 = x^2 + y^2 + (2xy + y^2)\omega$, dann ist festzustellen, ob die simultanen Kongruenzen:

$$x^2 + y^2 \equiv 0,\ (4)$$
$$y^2 + 2xy \pm 1 \equiv 0,\ (4)$$

für den Wert $+1$ oder -1 im letzten Ausdruck durch ganze rationale Zahlen x, y lösbar sind. Man erkennt leicht, daß zur Erfüllung der zweiten Kongruenz für den Wert -1 die Zahl y ungerade und x gerade sein müßte; dann ist aber $x^2 + y^2 \equiv y^2 \not\equiv 0$, (4). Ferner müßten für den Wert $+1$ in der letzten Kongruenz die beiden ganzen Zahlen x, y ungerade sein, dann ist aber $x^2 + y^2 \equiv 2 \not\equiv 0$, (4).

Mit einer andern Schlußweise, welche auch auf den allgemeinen Fall ohne weiteres paßt, könnte man dasselbe Resultat erhalten: Angenommen, es würde für die Grundeinheit ε eine der zwei Kongruenzen $\pm\varepsilon \equiv \alpha^2$, (4) gelten, so wäre auch $\pm\varepsilon' \equiv \alpha'^2$, (4), und folglich $\varepsilon\varepsilon' \equiv (\alpha\alpha')^2$, (4), oder $(\alpha\alpha')^2 \equiv -1$, (4). Weil aber $\alpha\alpha'$ jedenfalls eine rationale ganze Zahl darstellt, ist diese letzte Kongruenz sicher nicht möglich und die Annahme $\pm\varepsilon \equiv \alpha^2$, (4) unzulässig.

Der Körper $K(\sqrt{\pm\omega})$ ist also nicht unverzweigt in bezug auf den Körper $k(\sqrt{5})$, ebensowenig ist der Körper $K(\sqrt{-1})$ unverzweigt, da eine Kongruenz $-1 \equiv \alpha^2$, (4) nicht erfüllbar sein kann. In der Tat ist sogar gleich allgemein wegen $n(\varepsilon) = -1$, stets $m \equiv 1$, (4) oder $m \equiv 2$, (4), und es hätte darum die Kongruenz $-1 \equiv \alpha^2$, (4) stets eine Kongruenz $-1 \equiv x^2$, (4) für eine ganze rationale Zahl x zur Folge; eine solche kann aber durch eine ganze rationale Zahl nicht lösbar sein.

Ist andererseits $k(\sqrt{m})$ ein Körper mit der Klassenanzahl $h = 1$ resp. $\bar{h} = 2$, dessen Grundeinheit ε die Norm $+1$ besitzt, so existiert dazu sicher ein Klassenkörper. Wenn $m \equiv 1$ oder $m \equiv 2$, (4) ist und keinen quadratischen Faktor enthält, dann setze man: $\varepsilon = \frac{\alpha}{\alpha'}$. Zunächst ist $\varepsilon = \frac{1+\varepsilon}{1+\varepsilon'}$, man erkennt aber leicht, daß man $\alpha = \frac{1+\varepsilon}{t}$ stets so wählen kann, daß α und somit auch α' ganze Zahlen relativ prim zu der Zahl 2 sind. Es wird folglich $\varepsilon\alpha'^2 = \alpha\alpha'$, und da nun $\alpha\alpha'$ eine ungerade rationale Zahl ist, so wird stets eine der beiden Kongruenzen $\pm\alpha\alpha' \equiv 1$, (4) bestehen können, d. h. aber für $\varepsilon\alpha'^2$ gilt die Kongruenz $\pm\varepsilon\alpha'^2 \equiv \nu_1^2$ (4). Wegen der Voraussetzung über α', daß es nämlich relativ prim zu 2 sein soll, ergibt sich hieraus sofort auch

$\pm \varepsilon \equiv \nu^2, (4)$. Also bestimmt $\mu = \pm \varepsilon$ einen unverzweigten relativquadratischen Körper. Falls $m \equiv 3, (4)$ ist, bestimmt schon $\mu = -1$ einen solchen Körper, da alsdann stets $-1 \equiv (\sqrt{m})^2, (4)$ ausfällt.

4. Beispiel. Grundkörper $k(\sqrt{7})$. Hierfür ist $h = 1$, $\varepsilon = 8 + 3\sqrt{7}$, $n(\varepsilon) = +1$ und $\bar{h} = 2$. Im engeren Sinne existieren zwei Idealklassen, und zwar gehören zur Hauptklasse die Primideale: $(3 \pm \sqrt{7})$, (5), (11), (13), $17)$, (23), $(6 \pm \sqrt{7})$, usw., ferner zur Nichthauptklasse die Primideale: $(3 \pm 2\sqrt{7})$ $(9 \pm 4\sqrt{7})$, $(4 \pm 3\sqrt{7})$ usw.

Die Primideale der ersten Klasse sind entweder rationale Primzahlen, bezw. durch die Zerlegung der Primzahl $p = 2$, oder von Primzahlen p der Form $p \equiv 1, (4)$ entstanden.

Für die Primideale $\mathfrak{p}$ der Nichthauptklasse ist dagegen, falls $\mathfrak{p}\mathfrak{p}' = p$ gesetzt wird, $p \equiv 3, (4)$.

Nun ist $-1 \equiv (\sqrt{7})^2, (4)$, es bestimmt daher $\mu = -1$ einen unverzweigten relativquadratischen Körper. Bezeichnet ferner $\mathfrak{p}$ ein zu 2 primes Ideal der Nichthauptklasse und setzt man $(\pi) = \mathfrak{p}^2$, so bestimmt nach den Sätzen von Herrn Hilbert auch $\mu = \pm \pi$ stets einen Körper der verlangten Art. Wir betrachten einmal $K(\sqrt{-1})$. Als eine Basis dieses Relativkörpers kann man wählen:

$$1, \quad \omega = \sqrt{7}, \qquad \Omega = \frac{\sqrt{7} + \sqrt{-1}}{2}, \qquad \Omega_1 = \sqrt{7}\,\frac{\sqrt{7} + \sqrt{-1}}{2}.$$

$\varepsilon = 8 + 3\sqrt{7}$ ist eine Einheit des Körpers $k(\sqrt{7})$, gleichzeitig ist sie die Norm von:

$$\mathsf{E} = \frac{(3 + \sqrt{7})(1 - \sqrt{-1})}{2},$$

es ist also E eine Einheit des Relativkörpers.

Nach jedem Primideal der ersten Klasse gilt eine Kongruenz $-1 \equiv \alpha^2, (\mathfrak{p})$, dagegen ist diese Kongruenz nach Primidealen der zweiten Klasse nicht erfüllt. Die Primideale der ersten Klasse zerfallen im Relativkörper in das Produkt zweier Primideale; die Primideale der zweiten Klasse aber bleiben auch im Relativkörper Primideale.

Man findet leicht folgende Zerlegungen für die Ideale der Hauptklasse:

$$(3 + \sqrt{7}) = (1 + \sqrt{-1})(5 + 2\omega - 3\Omega - \Omega_1)$$
$$(5) = (2 + \sqrt{-1})(2 - \sqrt{-1}) = (2 - \omega + 2\Omega)(2 + \omega - 2\Omega)$$
$$(11) = (2 + \sqrt{-7})(2 - \sqrt{-7}) = (-5 + 2\Omega_1)(9 - 2\Omega_1)$$

$$(13) = (3 + 2\sqrt{-1})(3 - 2\sqrt{-1})$$
$$(17) = (4 + \sqrt{-1})(4 - \sqrt{-1})$$
$$(23) = (4 + \sqrt{-7})(4 - \sqrt{-7})$$
$$(6 + \sqrt{7}) = (3 + 2\omega - 3\Omega - \Omega_1)(3 + 2\omega - 3S(\Omega) - S(\Omega_1)),\ \text{usw.}$$

Die Primideale der zweiten Klasse bleiben Primideale, sie werden aber Ideale der Hauptklasse, weil z. B.:

$$(3 + 2\sqrt{7}) = (3\sqrt{-1} + 2\sqrt{-7}),$$

usw. geschrieben werden kann.

Ähnlich wie im Falle imaginärer Körper beweist man, daß der Körper $K(\sqrt{-1})$ eine ungerade Klassenanzahl im engeren Sinne besitzt.

Der Körper $K(\sqrt{-1})$ ist wieder ein Klassenkörper des Körpers $k(\sqrt{7})$, ebenso jeder der oben angeführten Körper $K(\sqrt{\pm\pi})$; denn diese Körper besitzen die Eigenschaften, die früher als charakteristisch für den Klassenkörper bezeichnet wurden.

Für den weiteren Fall, wo $m \equiv 2$, (4) ist, mag es genügen, als Beispiel den Körper $k(\sqrt{6})$ anzuführen. Da für denselben

$$h = 1, \quad \varepsilon = 5 - 2\sqrt{6}, \quad n(\varepsilon) = +1,$$

also $\bar{h} = 2$ ist, so müssen relativ quadratische unverzweigte (Klassen-) Körper existieren. Man sieht leicht, daß in der Tat:

$$K(\sqrt{-5 + 2\sqrt{6}}) = K(\sqrt{-\varepsilon})$$

ein solcher Relativkörper ist.

Ein letztes Beispiel soll endlich die Verhältnisse für einen Körper mit der Klassenanzahl $h = \bar{h} = 2$ erläutern. Ich beschränke mich auf die Anführung der Resultate und verweise übrigens auf die Note von Herrn Hilbert.

5. Beispiel. Grundkörper $k(\sqrt{10})$ mit der Klassenanzahl

$$h = \bar{h} = 2.$$

Man wähle irgend ein zu 2 primes Primideal, das nicht der Hauptklasse angehört, z. B. $\mathfrak{p} = (3,\ 2 + \sqrt{10})$, und bilde

$$(\pi) = \mathfrak{p}^2 = (-1 + \sqrt{10}).$$

Bezeichnet ε die Grundeinheit des Körpers, dann ergibt sich aus den allgemeinen Sätzen des Herrn Hilbert, daß eine der beiden Kongruenzen $\pm\varepsilon\pi \equiv \alpha^2$, (4) stets durch eine ganze Zahl α des Körpers $k(\sqrt{10})$ befriedigt werden kann. In der Tat wird $\mu = \varepsilon\pi = 7 + 2\sqrt{10} \equiv (1 + \sqrt{10})^2$, (4). Es ist somit $K(\sqrt{7 + 2\sqrt{10}})$ ein in

bezug auf $k(\sqrt{10})$ relativ quadratischer *unverzweigter* Körper. Als eine Basis dieses Relativkörpers kann man wählen:

$$1,\ \omega=\sqrt{10},\ \Omega=\frac{3(1+\sqrt{10})+\sqrt{\mu}}{2},\quad \Omega_1=(2-\sqrt{10})\frac{3(1+\sqrt{10})+\sqrt{\mu}}{6}.$$

Ferner sind $\mathsf{E}=\frac{1+\sqrt{10}+\sqrt{\mu}}{2}$ und $\mathsf{H}=1+\mathsf{E}$ Einheiten in $K(\sqrt{\mu})$, und zwar ist $N_k(\mathsf{E})=+1$, $N_k(\mathsf{H})=3+\sqrt{10}=\varepsilon$.

Nach der Ableitung der Zahl μ liegt die Vermutung nahe, daß das Ideal $(3,\ 2+\sqrt{10})$ im Körper $K(\sqrt{\mu})$ ein Hauptideal ist. Man findet auch leicht die Relationen:

$$(3)=(\sqrt{\mu})(20-4\omega+\Omega+5\Omega_1)=(\sqrt{\mu})(\mathsf{A}_1),$$

$$(2+\sqrt{10})=(\sqrt{\mu})(34-11\omega-4\Omega-10\Omega_1)=(\sqrt{\mu})(\mathsf{B}),$$

und:

$$(3,\ 2+\sqrt{10})=(\sqrt{\mu}).$$

Aus den Zerlegungen für 3 und $2+\sqrt{10}$ ergibt sich weiter die Gleichung:

$$(2,\ \sqrt{10})=(\mathsf{B})\quad\text{und}\quad(2)=(\mathsf{B})^2,$$

hieraus dann ferner:

$$(\sqrt{10})=(\mathsf{B})\,(25+7\omega-6\Omega+4\Omega_1)=(\mathsf{B})\,(\mathsf{B}_1)$$

$$(5)=(3-\sqrt{10})^2(\mathsf{B}_1)^2=(\Gamma)^2=(\mathsf{B}_1)^2,$$

wo

$$\Gamma=(25+7\omega-6\Omega+4\Omega_1)(3-\sqrt{10})$$

gesetzt ist.

Mit Hilfe der beiden Zahlengleichungen $2=\mathsf{B}^2$, und $5=\Gamma^2$ können wir nun leicht an Zahlenbeispielen die Zerlegungsgesetze im Relativkörper erläutern.

Bezeichnet (p) ein Hauptprimideal des Körpers $k(\sqrt{10})$, so fällt $\left(\frac{10}{p}\right)=-1$ aus. Diese Gleichung ist erfüllt entweder, wenn sich $\left(\frac{2}{p}\right)=+1, \left(\frac{5}{p}\right)=-1$ oder, wenn sich $\left(\frac{2}{p}\right)=-1$ $\left(\frac{5}{p}\right)=+1$ ergibt. Dann ist aber bezw. eine der beiden Gleichungen:

$$p=x^2-2y^2$$

resp.

$$p=x^2-5y^2$$

in ganzen rationalen Zahlen x, y lösbar, oder es gelten im Relativkörper bezw. die Zerlegungen:

$$(p) = (x - \mathsf{B}y)(x + \mathsf{B}y) \quad \text{oder} \quad (p) = (x - \Gamma y)(x + \Gamma y).$$

So ist z. B.:

$$\begin{aligned}
7 &= 3^2 - 2 \,.\, 1^2, & (7) &= (3 - \mathsf{B})(3 + \mathsf{B}),\\
11 &= 16 - 5 & (11) &= (4 - \Gamma)(4 + \Gamma),\\
17 &= 5^2 - 2 \,.\, 2^2, & (17) &= (5 - 2\mathsf{B})(5 + 2\mathsf{B}),\\
19 &= 12^2 - 5 \,.\, 5^2, & (19) &= (12 - 5\Gamma)(12 + 5\Gamma).
\end{aligned}$$

Bezeichnet p eine Primzahl, welche im Körper $k(\sqrt{10})$ zerfällt, indem $\left(\frac{10}{p}\right) = +1$ ist, dann hat man die zwei Möglichkeiten, daß $\left(\frac{2}{p}\right) = +1$, $\left(\frac{5}{p}\right) = +1$, oder $\left(\frac{2}{p}\right) = -1$, $\left(\frac{5}{p}\right) = -1$ ausfällt. Im ersteren Fall, wo gleichzeitig $\left(\frac{2}{p}\right) = +1$ $\left(\frac{5}{p}\right) = +1$ ist, muß die Zahl p in $k(\sqrt{m})$ notwendig in das Produkt zweier Hauptideale zerfallen; denn der Körper $k(\sqrt{10})$ hat zwei Geschlechter mit je einer Klasse, und die Faktoren von (p) gehören zum Hauptgeschlecht. Es gilt also eine Gleichung von der Form:

$$(p) = (x + \sqrt{10}\,y)(x - \sqrt{10}\,y).$$

Weil aber alsdann $p = x^2 - 2y^2$ und $p = x_1{}^2 - 5y_1{}^2$ ist, so ist p im Relativkörper durch vier verschiedene Ideale $(x + \sqrt{2}\,y)$ usw. teilbar. Jedes der beiden Hauptideale $x + \sqrt{10}\,y$ sowie $x - \sqrt{10}\,y$ muß selbst das Produkt aus je zwei Primidealen des Relativkörpers sein. Das Verhalten der Primfaktoren von p mögen wieder einige Beispiele erläutern:

Die Primzahlen p, für welche $\left(\frac{2}{p}\right) = +1$, $\left(\frac{5}{p}\right) = +1$ ausfällt, sind von den Formen $40n \pm 1$ und $40n \pm 9$. Man findet z. B.:

$$31 = 11^2 - 10 \,.\, 3^2 = (11 - 3\sqrt{10})(11 + 3\sqrt{10}) = \mathfrak{p}' \,.\, \mathfrak{p}$$

$$\mu \equiv 4, \ (\mathfrak{p}') \qquad \text{und} \qquad \mu \equiv 14^2, \ (\mathfrak{p})$$

$$\frac{11 - 3\sqrt{10}}{3 - \sqrt{10}} = (2 - \sqrt{\mu})(2 + \sqrt{\mu})$$

also als Idealgleichung:

$$(11 - 3\sqrt{10}) = (2 - \sqrt{\mu})(2 + \sqrt{\mu}),$$

und außerdem:

$$(11 + 3\sqrt{10}) = \left(-1 + \sqrt{10} + 2\frac{(2 - \sqrt{10})\sqrt{\mu}}{3}\right)\left(-1 + \sqrt{10} - 2\frac{(2 - \sqrt{10})\sqrt{\mu}}{3}\right).$$

Ferner ist:

$$41 = 9^2 - 10 \,.\, 2^2 = (9 - 2\sqrt{10})(9 + 2\sqrt{10}) = \mathfrak{p}' \,.\, \mathfrak{p},$$

$$\mu \equiv 4^2, \ (\mathfrak{p}') \quad \text{und} \quad \mu \equiv 11^2, \ (\mathfrak{p})$$

und

$$(9 - 2\sqrt{10}) = (4 - \sqrt{\mu})(4 + \sqrt{\mu})$$

$$(9 + 2\sqrt{10}) = \left(8 + 2\sqrt{10} + \frac{(5 + 2\sqrt{10})\sqrt{\mu}}{3}\right)\left(8 + 2\sqrt{10} - \frac{(5 + 2\sqrt{10})\sqrt{\mu}}{3}\right).$$

Ferner

$$79 = 13^2 - 10 \,.\, 3^2 = (13 - 3\sqrt{10})(13 + 3\sqrt{10}) = \mathfrak{p}' \,.\, \mathfrak{p}$$

und

$$\mu \equiv 11^2, \ (\mathfrak{p}'), \quad \mu \equiv 29^2, \quad (\mathfrak{p})$$

$$(13 - 3\sqrt{10}) = \left(-2 - \sqrt{10} + \frac{(-5 + \sqrt{10})\sqrt{\mu}}{3}\right)\left(-2 - \sqrt{10} - \frac{(-5 + \sqrt{10})\sqrt{\mu}}{3}\right)$$

$$(13 + 3\sqrt{10}) = \left(-2 + \sqrt{10} + \frac{(+5 - \sqrt{10})\sqrt{\mu}}{3}\right)\left(-2 + \sqrt{10} - \frac{(5 - \sqrt{10})\sqrt{\mu}}{3}\right)$$

Endlich ist:

$$89 = 27^2 - 10 \,.\, 8^2 = (27 - 8\sqrt{10})(27 + 8\sqrt{10}) = \mathfrak{p}' \,.\, \mathfrak{p}.$$

Dann ist:

$$\mu \equiv 6^2 \ (\mathfrak{p}'); \quad \mu \equiv 44^2, \ (\mathfrak{p})$$

und:

$$(27 - 8\sqrt{10}) = \left(1 + 2\frac{(7 - 2\sqrt{10})\sqrt{\mu}}{3}\right)\left(1 - 2\frac{(7 - 2\sqrt{10})\sqrt{\mu}}{3}\right)$$

$$(27 + 8\sqrt{10}) = (1 + 2\sqrt{\mu})(1 - 2\sqrt{\mu}).$$

Wir müssen uns mit diesen Beispielen begnügen und wenden uns kurz zu den Primfaktoren eines Ideals (p) aus dem Grundkörper, wenn jetzt gleichzeitig $\left(\frac{2}{p}\right) = -1$, $\left(\frac{5}{p}\right) = -1$ ist. In diesem Fall gehören die Primfaktoren von (p) nicht dem Hauptgeschlecht und nicht der Hauptklasse an, sie sind Nichthauptideale. Da aber alsdann die Gleichung:

$$p = 2x^2 - 5y^2$$

stets in ganzen rationalen Zahlen x, y lösbar ist, so läßt (p) im Relativkörper die Zerlegung zu:

$$(p) = (\mathrm{B}x + \Gamma y)(\mathrm{B}x - \Gamma y),$$

und wir sahen schon, daß die Ideale $(2, \sqrt{10})$ und $(5, \sqrt{10})$ zu Hauptidealen wurden.

Beispielsweise ist:

$$\left(\frac{10}{13}\right) = +1, \quad \left(\frac{2}{13}\right) = -1, \quad \left(\frac{5}{13}\right) = -1$$

und

$$(13) = (13,\ 6 - \sqrt{10})(13,\ 6 + \sqrt{10}) = \mathfrak{p}'.\mathfrak{p}.$$

Es ist nicht möglich, die Kongruenz

$$\mu \equiv \alpha^2,\ (\mathfrak{p})$$

oder auch die Kongruenz:

$$\mu \equiv \alpha_1^2,\ (\mathfrak{p}')$$

durch eine ganze Zahl α_1 bezw. α' des Körpers $k(\sqrt{10})$ zu erfüllen. In der Tat ist:

$$\mu \equiv 8,\ (\mathfrak{p}) \quad \text{und} \quad \mu \equiv 6,\ (\mathfrak{p}'),$$

d. h. $\mathfrak{p}$ und $\mathfrak{p}'$ zerfallen im Relativkörper nicht. Man hat aber für den Relativkörper die Gleichungen:

$$(13,\ 6 + \sqrt{10}) = (3\,\mathrm{B} + \Gamma) \quad \text{und} \quad (13,\ 6 - \sqrt{10}) = (3\,\mathrm{B} - \Gamma)$$

entsprechend der Gleichung: $13 = 2.9 - 5$.

Analog ist:

$$(37) = (37,\ 11 - \sqrt{10})(37,\ 11 + \sqrt{10}) = \mathfrak{p}'.\mathfrak{p}$$

$$\mu \equiv 22,\ (\mathfrak{p}); \quad \mu \equiv 29,\ (\mathfrak{p}');$$

und im Relativkörper wird:

$$\mathfrak{p} = \mathfrak{P} = (9\mathrm{B} + 5\Gamma), \qquad \mathfrak{p}' = \mathfrak{P}_1 = (9\mathrm{B} - 5\Gamma).$$

Diejenigen Primideale des Grundkörpers, welche nicht Hauptideale sind, bleiben im Oberkörper $K(\sqrt{\mu})$ Primideale, sie werden aber zu Hauptidealen.

Ähnlich wie für den Fall eines imaginären Grundkörpers beweist man noch, daß die Klassenanzahl des Relativkörpers $K(\sqrt{\mu})$ ungerade ist.

Gerade die Tatsache, daß die Klassenanzahl des Klassenkörpers ungerade ist, erlaubt die Verwendung des Klassenkörpers zur Aufstellung des quadratischen Reziprozitätsgesetzes im Grundkörper.

Die einfachen Sätze über die Existenz des Klassenkörpers für quadratische Grundkörper lassen sich erweitern, wenn man Relativkörper vom vierten und von höherem Grad betrachtet. Nehmen wir als Beispiel etwa den Grundkörper $k(\sqrt{-14})$ mit der Klassenanzahl $h = 4$. Die Klassen dieses Körpers lassen sich durch $(1), (2, \sqrt{-14}), (3, 1 - \sqrt{-14}), (3, 1 + \sqrt{-14}) = \mathfrak{r}$ oder $\mathfrak{r}, \mathfrak{r}^2, \mathfrak{r}^3, \mathfrak{r}^4 \sim 1$ darstellen. Setzt man

$$\mathfrak{r} = (3, 1 + \sqrt{-14}) \quad \text{und} \quad (\varrho) = \mathfrak{r}^4 = (5 + 2\sqrt{-14}),$$

so verifiziert man leicht die Kongruenz:

$$-\varrho = -5 - 2\sqrt{-14} \equiv (1 + \sqrt{-14})^2, \quad (4)$$

und folgert dann, daß $K\sqrt{-5-2\sqrt{-14}} = K(\sqrt{\mu})$ ein zu $k(\sqrt{-14})$ relativ quadratischer und relativ unverzweigter Körper ist. Für diesen Körper bilden die Zahlen:

$$1, \ \omega = \sqrt{-14}, \quad \Omega = 9\,\frac{9(1+\sqrt{-14}) + \sqrt{\mu}}{18},$$

$$\Omega_1 = (2 + \sqrt{-14})\,\frac{9(1+\sqrt{-14}) + \sqrt{\mu}}{18}$$

eine Basis. Man erkennt leicht, daß die Ideale:

$$\mathfrak{p}_2 = (2, \sqrt{-14}), \quad \mathfrak{p}_3 = \mathfrak{r} = (3, 1 + \sqrt{-14})$$

und

$$\mathfrak{p}_3' = \mathfrak{r}' = (3, 1 - \sqrt{-14})$$

im Relativkörper nicht zerfallen. Es werden:

$$\mathfrak{p}_2 = \mathfrak{P} = (12 - 3\sqrt{-14} + 2\Omega_1)$$

$$\mathfrak{r}^2 = (\sqrt{\mu})$$

zu Hauptidealen, dagegen bleiben $\mathfrak{r}$ und $\mathfrak{r}'$ auch im Relativkörper Nichthauptideale. Daraus folgt schon, daß die Klassenanzahl des Relativkörpers noch gerade ist. Um zum Klassenkörper für $k(\sqrt{-14})$ zu gelangen, müßte man einen Oberkörper wählen, der in Bezug auf $k(\sqrt{-14})$ vom vierten Grade ist.

Diese Untersuchungen führen aber weit über den Rahmen dieses Buches hinaus. Wir müssen uns mit der Andeutung der Probleme begnügen, da wir das Ziel unserer Darstellung erreicht haben.

Erklärungen zu den Tabellen und Bemerkungen über die Auflösung der Pellschen Gleichung.

Wie die darstellende Geometrie eine Ergänzung zur abstrakten Theorie der Geometrie bildet, aus welcher jeder, der ihre Methoden zu gebrauchen weiß, neue Anregung und das Gefühl der Sicherheit ernten wird, so hat auch die Zahlentheorie ihre angewandte Richtung in der numerischen Rechnung. Ebenso wie das Zeichnen geometrischer Formen und die bildliche Darstellung geometrischer Sätze, so gewährt das Zahlenrechnen einen großen Reiz dem, der die allgemeine Theorie aufgefaßt hat. Ja, der Anfänger wird eine völlige Klarheit über seinen Besitz nur durch die Anwendung auf Beispiele erlangen, und auch der Fortgeschrittene wird aus der Zahlenrechnung viele neue Anregung ziehen, sind doch sogar fast alle wichtigen Sätze der Zahlentheorie auf dem Wege der Induktion gefunden worden.

Zur Erleichterung sowie zur Kontrolle solcher Rechnungen können die Tabellen dienen, welche den Schluß des Buches bilden. Dieselben sind gleichzeitig als eine Tafel der Klassenanzahlen aller quadratischen Zahlkörper mit quadratfreier Grundzahl zwischen -97 und $+101$ gedacht.

Die *Einrichtung* der Tabellen ist wohl ohne weiteres verständlich. Zunächst enthalten dieselben zwei große Abteilungen für die imaginären Körper und für die reellen Körper, mit einander ähnlichen Einteilungen.

Die vertikalen Kolonnen sind für die imaginären Körper so angenommen, daß die Kolonnen der Reihe nach enthalten:

1.) die Grundzahl des Körpers;

2.) die einfachste Basis des Körpers, aus welcher alle übrigen durch eine lineare Substitution abgeleitet werden können;

3.) die Diskriminante des Körpers in ihre, der Größe nach geordneten, Primfaktoren zerlegt;

4.) die sämtlichen, einander nicht äquivalenten Ideale des Körpers, deren Norm $< |\sqrt{d}|$ ist;

5.) die Aufzählung der Klassen, dargestellt in der Form $K^k . L^l \ldots$, durch eine möglichst kleine Anzahl von Grundklassen. Der Buchstabe A soll hierbei andeuten, daß eine Klasse ambig ist. Wenn die sämtlichen Klassen eines Körpers sich durch die aufeinanderfolgenden Potenzen *einer* Klasse J oder A darstellen lassen, so heißt der Körper *zyklisch*. Die nicht zyklischen Körper der Tabelle sind Abelsche Körper. Ihre sämtlichen Klassen lassen sich durch die Potenzen und Produkte von zwei geeignet ausgewählten Klassen darstellen.

Außer den durch A bezeichneten Klassen sind noch diejenigen in der Tabelle leicht aufzufindenden Klassen ambig, deren Quadrat die Hauptklasse liefert. Ideale und Klassen, die auf gleicher Linie stehen, gehören zusammen, es kann stets das betreffende Ideal als Vertreter der Klasse genommen werden;

6.) die Einteilung der Klassen in Geschlechter; die Klassen, welche zu einem Geschlecht gehören, sind durch geschwungene Klammern zusammengefaßt;

7.) die Charakterensysteme der Geschlechter. Nach Nr. 28, S. 140ff., besteht jedes Charakterensystem aus einer Anzahl positiver oder negativer Einheiten $+1, -1$. In der Tabelle ist nur $+, -$ geschrieben, und zwar beziehen sich diese Vorzeichen von links nach rechts auf die der Größe nach geordneten Primfaktoren der Diskriminante, also auf die in der dritten Kolonne ebenso von links nach rechts aufeinanderfolgenden Primzahlen.

Für die reellen Körper treten zu den aufgezählten Kolonnen noch zwei weitere hinzu: die mit ε überschriebene enthält jedesmal diejenige Grundeinheit des Körpers, für welche $|\varepsilon| > 1$ ist, und die mit $n(\varepsilon)$ überschriebene gibt die Norm der Grundeinheit. Ferner ist jetzt die Berechnung des Charakterensystems abweichend von jener für die imaginären Körper. Wenn m eine positive Zahl bezeichnet, welche durch Primzahlen von der Form $q \equiv 3, (4)$ teilbar ist, so wird:

$$\left(\frac{-1,\, m}{q}\right) = -1.$$

Wenn nun $\mathfrak{j}$ ein Ideal des Körpers bedeutet, dann wird $\bar{n} = \pm n(\mathfrak{j})$ derart angenommen, daß für einen *bestimmten* dieser Primfaktoren q das Symbol $\left(\frac{\bar{n},\, m}{q}\right) = +1$ ausfällt. Es brauchen daher bei der Aufstellung des Charakterensystems eines Ideals $\mathfrak{j}$ nur noch die von dem gewählten q verschiedenen Primfaktoren von d berücksichtigt zu werden.

Bei der Angabe von d in der dritten Kolonne sind nun die Primfaktoren von d so aufgeführt, daß zunächst die Zahl $q \equiv 3, (4)$ angeschrieben ist, welche zur Bestimmung des Vorzeichens in $\bar{n} = \pm n(\mathfrak{j})$ benützt wurde (falls m eine solche Primzahl enthält), dann folgen die übrigen Primfaktoren von d wieder der Größe nach geordnet.

Die Kolonne für die Charakterensysteme gibt alsdann die Werte $\left(\frac{\bar{n}, m}{p}\right)$ für die ebenfalls der Größe nach geordneten Primfaktoren p, q der Diskriminante, *abgesehen* eben von dem ausgesonderten Faktor q.

Die *Berechnung* der Tafeln ist sehr einfach, weil man bald einen Überblick über die wichtigen Punkte gewinnt und zu kleinen Kunstgriffen geführt wird. Um die Ideale aufzustellen, berechnet man zunächst das Symbol $\left(\frac{d}{p}\right)$ für alle Primzahlen $p < |\sqrt{d}|$ und setzt dann eventuell die Primideale $\mathfrak{p}$, $\mathfrak{p}'$ usw. in der Form $(p, a + \omega)$ an. Um zu entscheiden, ob zwei in i bezw. h aufgehende Ideale $\mathfrak{j}$ und $\mathfrak{h}$ äquivalent sind, bildet man $\mathfrak{j}'\mathfrak{h}$ und untersucht, ob dies ein Hauptideal ist, indem man nachsieht, ob sämtliche Zahlen des Ideals einen gemeinsamen Faktor enthalten, bezw. ob die Gleichung:

$$ih = x^2 - my^2 \quad \text{bezw.} \quad \pm ih = x^2 + xy + \frac{1-m}{4} y^2,$$

für ganze rationale Zahlen x, y lösbar ist. Die Entscheidung hierüber ist offenbar sehr leicht für imaginäre Körper, bei reellen Körpern vereinfacht sich die Überlegung meist dadurch, daß man umgekehrt verfährt, die Zahlen x, y selbst wählt und so die kleinsten Zahlen a aufstellt, für welche die Gleichung $a = x^2 - my^2$ usw. erfüllt ist.

Bei der Entscheidung darüber, ob ein bestimmtes Ideal Hauptideal ist oder nicht, kann man häufig von den Sätzen über die Geschlechter des Körpers Gebrauch machen. Wir haben dies an mehreren Beispielen in Nr. 55, vergl. S. 322, 334 usw., schon erläutert.

Eine ähnliche Aufgabe wie die eben angeführte ist die Bestimmung der Grundeinheit ε, d. h. die Auflösung der Diophantischen Gleichung:

$$x^2 - my^2 = +1, \quad \text{bezw.} \quad x^2 + xy + \frac{1-m}{4} y^2 = \pm 1$$

für positive m.

Es ist früher schon auf die Methoden hingewiesen worden zur Bestimmung der Lösungswerte dieser Gleichungen. Die allgemeine, stets brauchbare Methode beruht auf der Kettenbruchentwicklung von $\sqrt{m}$.

Man kann aber häufig auch die Sätze über die Geschlechter des Körpers und die Folgerungen daraus, Nr. 32, S. 164, sowie die Eigenschaften der ambigen Ideale zur Berechnung benützen, wie man am raschesten aus Beispielen ersieht.

1. $k(\sqrt{55})$. Nach den Bezeichnungen von S. 141 ist hier $t = 3$, $r = 2$ und daher $g = 2$. Der Körper enthält zwei ambige Klassen, auf welche sich die Ideale verteilen, die durch die Zerlegung der Zahlen 2, 5, 10, 11 entstehen. Weil nun das Ideal (2) zerlegbar ist, eine Kongruenz:

$$x^2 \pm 2 \equiv 0, \ (55)$$

aber nicht lösbar sein kann, so ist $(2, 1 + \sqrt{55})$ ein ambiges Ideal. Da ferner ebensowenig eine Kongruenz $x^2 \pm 10 \equiv 0$ (55) lösbar sein kann, so sind die in (2) bezw. (5) aufgehenden Primideale nicht äquivalent. Das ambige Ideal, welches durch die Zerlegung der Zahl 5 bestimmt wird, ist somit ein Hauptideal, oder das Ideal (5) ist gleich dem Quadrat eines Hauptideals.

In der Tat findet man:

$$5 = 15^2 - 55 \, . \, 4,$$

wo 15 und 2 die absolut kleinste Lösung der Gleichung $5 = x^2 - 55y^2$ darstellen. Weil andererseits 5 in ambige Ideale zerfällt, so ist:

$$(5) = (15 \pm 2\sqrt{55})^2.$$

Führt man rechts die Multiplikation aus, so folgt z. B. für das obere Zeichen:

$$(5) = (5)(89 + 12\sqrt{55}).$$

Es ist dann

$$\varepsilon = 89 + 12\sqrt{55}$$

eine Grundeinheit des Körpers.

2.) $k(\sqrt{31})$. Die Zahl 2 ist in d enthalten, also $(2) = \mathfrak{p}_2^2$.

Nun ist früher bewiesen worden, daß die Diophantische Gleichung:

$$2 = x^2 - 31y^2$$

lösbar sein muß. Aus der Kongruenz $x^2 - 2 \equiv 0$, (31) folgt dann, daß $x = 8 + 31\,u$ und

$$y^2 = 2 + 16\,u + 31\,u^2$$

wird, wo u eine ganze rationale Zahl bezeichnet.

Es ist nun diejenige ganze rationale Zahl u zu suchen, für welche die rechte Seite dieser letzten Gleichung eine Quadratzahl ist. Man findet leicht $y^2 = 49 = 7^2$ für $u = 1$ und daraus $x = 39$.

Somit erhält man:

$$\mathfrak{p}_2 = (39 + 7\sqrt{31})$$

und

$$(2) = (1521 + 1519 + 2.273\sqrt{31}) = \mathfrak{p}_2^2,$$

resp.

$$(2) = (2)(1520 + 273\sqrt{31}).$$

Nun ist die gesuchte Einheit:

$$\varepsilon = 1520 + 273\sqrt{31}.$$

3.) $k(\sqrt{67})$. Die Zerlegung der Zahl 2 muß auf ein ambiges Hauptideal führen, da der Körper nur eine ambige Klasse, die Hauptklasse selbst, enthält. Es muß also die Diophantische Gleichung:

$$-2 = x^2 - 67y^2$$

lösbar sein. Man findet aus der Kongruenz $x^2 + 2 \equiv 0$, (67) leicht:

$$x = 20 + 67u, \qquad y^2 = 6 + 40u + 67u^2.$$

Die zweite dieser Gleichungen ist befriedigt für $u = 3$, also wird:

$$(2) = (221 + 27\sqrt{67})^2,$$

und hieraus folgt durch Ausquadrieren:

$$\varepsilon = 48\,842 + 5967\sqrt{67}$$

4.) $k(\sqrt{93})$. In diesem Körper ist z. B. $(3) = \mathfrak{p}_3^2$, und da nur eine ambige Klasse existiert, so ist $\mathfrak{p}_3$ Hauptideal. In der Tat findet man sehr rasch, daß:

$$(3) = (4 + \omega)(4 + \omega'),$$

also auch

$$(3) = (4 + \omega)^2$$

ist, woraus man weiter als Grundeinheit entnimmt:

$$\varepsilon = 13 + 3\omega.$$

Nach den Tabellen ist $k(\sqrt{94})$ derjenige Körper, dessen Grundeinheit die größten Zahlen 2 143 295 und 221 064 enthält. Auch diese Zahlen zu bestimmen, ist eine sehr kurze Arbeit, wenn man wieder bedenkt, daß die Gleichung $2 = x^2 - 94y^2$ lösbar sein muß. Es wird dann $(2) = (\alpha)^2$ und danach erhält man ε wie in den übrigen Fällen.

In allen den bisherigen Beispielen ergibt sich ein Ansatz zur Lösung der Gleichung:

$$x^2 - my^2 = +1 \quad \text{oder} \quad x^2 + xy + \frac{1-m}{4} y^2 = \pm 1 \tag{1}$$

dadurch, daß man zuerst ein von $(\sqrt{m})$ *verschiedenes ambiges Hauptideal des Körpers aufsucht und dann aus dem Quadrat dieses Hauptideals die Grundeinheit* ε *entnimmt. Es werden so stets die Lösungswerte der Gleichungen* (1) *aus der Lösung der Gleichung:*

$$x^2 - my^2 = \pm a, \qquad x^2 + xy + \frac{1-m}{4} y^2 = \pm a,$$

wo a *ein Faktor von* $4m$ *oder* m *ist, abgeleitet, und diese letzteren Werte sind stets viel kleiner als die gesuchten.*

Dieses Hilfsmittel versagt aber ganz in Fällen wie $k(\sqrt{73})$, $k(\sqrt{97})$ usw., wo die Grundzahl eine Primzahl von der Form $m \equiv 1, (4)$ ist, oder für $k(\sqrt{65})$, $k(\sqrt{85})$ usw., denn diese Körper enthalten ja nur $(\sqrt{73})$ bezw. $(\sqrt{97})$ bezw. $(\sqrt{m})$, ferner $(\sqrt{65})$, $(\sqrt{85})$ selbst als ambige Hauptideale. Hat man aber z. B. in dem Fall, wo m Primzahl ist, festgestellt, daß ein Ideal (a) gleich dem Produkt zweier konjugierter Hauptideale ist, so kann man die einfachsten *Zahlen* α, α_1 bestimmen, für welche:

$$+a = \alpha . \alpha' \quad \text{und} \quad -a = \alpha_1 . \alpha_1'$$

wird, da ja dann $n(\varepsilon) = -1$ ist; dann wird entweder:

$$\varepsilon = \frac{\alpha}{\alpha_1} \qquad \text{oder} \qquad \varepsilon = \frac{\alpha}{\alpha_1'}.$$

Z. B. ergibt sich für den Körper $k(\sqrt{97})$ sehr leicht:

$$+2 = (38 - 7\omega)(38 - 7\omega')$$
$$-2 = (146 + 33\omega)(146 - 33\omega'),$$

und hieraus folgt:

$$\varepsilon = \frac{146 + 33\omega}{38 - 7\omega} = 5035 + 1138\omega.$$

Für die Körper $k(\sqrt{65})$ und $k(\sqrt{85})$ ist die Berechnung der Grundeinheit überhaupt nicht schwer, man hat aber auch hier sofort einen ersten Ansatz, da $n(\varepsilon) = -1$ werden muß.

Jedenfalls kann man häufig weitläufige Rechnungen durch kleine Überlegungen abkürzen, die allgemeine Theorie liefert in den meisten Fällen irgend einen Ansatz zur Erleichterung des Zahlenrechnens und erfüllt so eine Anforderung, welche im Grunde das letzte Ziel aller allgemeinen Theorien ist.

Tabellen.

Imaginäre Körper.

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakteren-system
-1 *)	$\sqrt{-1}$	-2^2	(1)	1	1	$+$
-2	$\sqrt{-2}$	-2^3	(1)	1	1	$+$
-3 **)	$\frac{1+\sqrt{-3}}{2}$	-3	(1)	1	1	$+$
-5	$\sqrt{-5}$	$-2^2\cdot 5$	(1)	A^2	A^2	$+\ +$
			$(2,\ 1+\sqrt{-5})$	A	A	$-\ -$
-6	$\sqrt{-6}$	$-2^3\cdot 3$	(1)	A^2	A^2	$+\ +$
			$(2,\ \sqrt{-6})$	A	A	$-\ -$
-7	$\frac{1+\sqrt{-7}}{2}$	-7	(1)	1	1	$+$
-10	$\sqrt{-10}$	$-2^3\cdot 5$	(1)	A^2	A^2	$+\ +$
			$(2,\ \sqrt{-10})$	A	A	$-\ -$
-11	$\frac{1+\sqrt{-11}}{2}$	-11	(1)	1	1	$+$
-13	$\sqrt{-13}$	$-2^2\cdot 13$	(1)	A^2	A^2	$+\ +$
			$(2, 1+\sqrt{-13})$	A	A	$-\ -$
-14	$\sqrt{-14}$	$-2^3\cdot 7$	(1)	J^4	J^4 ***)	$+\ +$
			$(3, 1-\sqrt{-14})$	J^3	J^2	
			$(2,\ \sqrt{-14})$	J^2	J^3	$-\ -$
			$(3, 1+\sqrt{-14})$	J	J	

*) Dieser Körper enthält die Einheiten $\pm\sqrt{-1}$ außer ± 1.

**) Dieser Körper enthält außer ± 1 als Einheiten noch $\pm\omega$, $\pm\omega'$.

***) In den beiden Rubriken: Klassen und Geschlechter, stimmen die Anordnungen der Klassen nicht überein!

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakteren-system
-15	$\frac{1+\sqrt{-15}}{2}$	$-3\cdot 5$	(1) $(2,\ 1+\omega)$	A^2 A	A^2 A	$+\ +$ $-\ -$
-17	$\sqrt{-17}$	$-2^2\cdot 17$	(1) $(3,\ 1-\sqrt{-17})$ $(2,\ 1+\sqrt{-17})$ $(3,\ 1+\sqrt{-17})$	J^4 J^3 J^2 J	J^4 J^2 J^3 J	$+\ +$ $-\ -$
-19	$\frac{1+\sqrt{-19}}{2}$	-19	(1)	1	1	$+$
-21	$\sqrt{-21}$	$-2^2\cdot 3\cdot 7$	(1) $(5,\ 3+\sqrt{-21})$ $(3,\ \sqrt{-21})$ $(2,\ 1+\sqrt{-21})$	$A^2A_1^2$ AA_1 A_1 A	1 AA_1 A_1 A	$+\ +\ +$ $+\ -\ -$ $-\ +\ -$ $-\ -\ +$
-22	$\sqrt{-22}$	$-2^3\cdot 11$	(1) $(2,\ \sqrt{-22})$	A^2 A	A^2 A	$+\ +$ $-\ -$
-23	$\frac{1+\sqrt{-23}}{2}$	-23	(1) $(2,\ \omega')$ $(2,\ \omega)$	J^3 J^2 J	J^3 J^2 J	$+$
-26	$\sqrt{-26}$	$-2^3\cdot 13$	(1) $(5,\ 2-\sqrt{-26})$ $(3,\ 1+\sqrt{-26})$ $(2,\ \sqrt{-26})$ $(3,\ 1-\sqrt{-26})$ $(5,\ 2+\sqrt{-26})$	J^6 J^5 J^4 J^3 J^2 J	J^6 J^4 J^2 J^5 J^3 J	$+\ +$ $-\ -$
-29	$\sqrt{-29}$	$-2^2\cdot 29$	(1) $(3,\ 1-\sqrt{-29})$ $(5,\ 1-\sqrt{-29})$ $(2,\ 1+\sqrt{-29})$ $(5,\ 1+\sqrt{-29})$ $(3,\ 1+\sqrt{-29})$	J^6 J^5 J^4 J^3 J^2 J	J^6 J^4 J^2 J^5 J^3 J	$+\ +$ $-\ -$
-30	$\sqrt{-30}$	$-2^3\cdot 3\cdot 5$	(1) $(2,\ \sqrt{-30})$ $(3,\ \sqrt{-30})$ $(5,\ \sqrt{-30})$	$A^2A_1^2$ AA_1 A_1 A	$A^2A_1^2$ AA_1 A_1 A	$+\ +\ +$ $+\ -\ -$ $-\ +\ -$ $-\ -\ +$

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakteren-system
-31	$\frac{1+\sqrt{-31}}{2}$	-31	(1)	J^3	J^3	$+$
			$(2,\ 1+\omega')$	J^2	J^2	
			$(2,\ 1+\omega)$	J	J	
-33	$\sqrt{-33}$	$-2^2\cdot 3\cdot 11$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+\ +\ +$
			$(2, 1+\sqrt{-33})$	AA_1	AA_1	$+\ -\ -$
			$(3,\ \sqrt{-33})$	A_1	A_1	$-\ +\ -$
			$(6, 3+\sqrt{-33})$	A	A	$-\ -\ +$
-34	$\sqrt{-34}$	$-2^3\cdot 17$	(1)	J^4	J^4	$+\ +$
			$(5, 1-\sqrt{-34})$	J^3	J^2	
			$(2,\ \sqrt{-34})$	J^2	J^3	$-\ -$
			$(5, 1+\sqrt{-34})$	J	J	
-35	$\frac{1+\sqrt{-35}}{2}$	$-5\cdot 7$	(1)	A^2	A^2	$+\ +$
			$(5,\ \sqrt{-35})$	A	A	$-\ -$
-37	$\sqrt{-37}$	$-2^2\cdot 37$	(1)	A^2	A^2	$+\ +$
			$(2, 1+\sqrt{-37})$	A	A	$-\ -$
-38	$\sqrt{-38}$	$-2^3\cdot 19$	(1)	J^6	J^6	$+\ +$
			$(3, 1-\sqrt{-38})$	J^5	J^4	
			$(7, 2+\sqrt{-38})$	J^4	J^2	
			$(2,\ \sqrt{-38})$	J^3	J^5	$-\ -$
			$(7, 2-\sqrt{-38})$	J^2	J^3	
			$(3, 1+\sqrt{-38})$	J	J	
-39	$\frac{1+\sqrt{-39}}{2}$	$-3\cdot 13$	(1)	J^4	J^4	$+\ +$
			$(2,\ \omega')$	J^3	J^2	
			$(3,\ 1-2\omega)$	J^2	J^3	$-\ -$
			$(2,\ \omega)$	J	J	
-41	$\sqrt{-41}$	$-2^2\cdot 41$	(1)	J^8	J^8	$+\ +$
			$(3, 1-\sqrt{-41})$	J^7	J^6	
			$(5, 2-\sqrt{-41})$	J^6	J^4	
			$(7, 1-\sqrt{-41})$	J^5	J^2	
			$(2, 1+\sqrt{-41})$	J^4	J^7	$-\ -$
			$(7, 1+\sqrt{-41})$	J^3	J^5	
			$(5, 2+\sqrt{-41})$	J^2	J^3	
			$(3, 1+\sqrt{-41})$	J	J	

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakterensystem
-42	$\sqrt{-42}$	$-2^3 \cdot 3 \cdot 7$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+\ +\ +$
			$(7, \sqrt{-42})$	AA_1	AA_1	$+\ -\ -$
			$(3, \sqrt{-42})$	A_1	A_1	$-\ +\ -$
			$(2, \sqrt{-42})$	A	A	$-\ -\ +$
-43	$\frac{1+\sqrt{-43}}{2}$	-43	(1)	1	1	$+$
-46	$\sqrt{-46}$	$-2^3 \cdot 23$	(1)	J^4	J^4	$+\ +$
			$(5, 2-\sqrt{-46})$	J^3	J^2	
			$(2, \sqrt{-46})$	J^2	J^3	$-\ -$
			$(5, 2+\sqrt{-46})$	J	J	
-47	$\frac{1+\sqrt{-47}}{2}$	-47	(1)	J^5	J^5	$+$
			$(2, 1+\omega')$	J^4	J^4	
			$(3, \omega')$	J^3	J^3	
			$(3, \omega)$	J^2	J^2	
			$(2, 1+\omega)$	J	J	
-51	$\frac{1+\sqrt{-51}}{2}$	$-3 \cdot 17$	(1)	A^2	A^2	$+\ +$
			$(3, 1-2\omega)$	A	A	$-\ -$
-53	$\sqrt{-53}$	$-2^2 \cdot 53$	(1)	J^6	J^6	$+\ +$
			$(3, 1-\sqrt{-53})$	J^5	J^4	
			$(9, 1-\sqrt{-53})$	J^4	J^2	
			$(2, 1+\sqrt{-53})$	J^3	J^5	$-\ -$
			$(9, 1+\sqrt{-53})$	J^2	J^3	
			$(3, 1+\sqrt{-53})$	J	J	
-55	$\frac{1+\sqrt{-55}}{2}$	$-5 \cdot 11$	(1)	J^4	J^4	$+\ +$
			$(2, \omega')$	J^3	J	
			$(5, 1-2\omega)$	J^2	J^3	$-\ -$
			$(2, \omega)$	J	J	
-57	$\sqrt{-57}$	$-2^2 \cdot 3 \cdot 19$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+\ +\ +$
			$(2, 1+\sqrt{-57})$	AA_1	AA_1	$+\ -\ -$
			$(3, \sqrt{-57})$	A_1	A_1	$-\ +\ -$
			$(6, 3+\sqrt{-57})$	A	A	$-\ -\ +$
-58	$\sqrt{-58}$	$-2^3 \cdot 29$	(1)	A^2	A^2	$+\ +$
			$(2, \sqrt{-58})$	A	A	$-\ -$

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakterensystem
-59	$\frac{1+\sqrt{-59}}{2}$	-59	(1)	J^3	J^3	$+$
			$(3,\ \omega')$	J^2	J^2	
			$(3,\ \omega)$	J	J	
-61	$\sqrt{-61}$	$-2^2\cdot 61$	(1)	J^3	J^3	$+\ +$
			$(5, 2-\sqrt{-61})$	J^2	J^2	
			$(5, 2+\sqrt{-61})$	J	J	
			$(7, 3-\sqrt{-61})$	AJ^2	AJ^2	$-\ -$
			$(7, 3+\sqrt{-61})$	AJ	AJ	
			$(2, 1+\sqrt{-61})$	A	A	
-62	$\sqrt{-62}$	$-2^3\cdot 31$	1	J^8	J^8	$+\ +$
			$(3, 1-\sqrt{-62})$	J^7	J^6	
			$(7, 1+\sqrt{-62})$	J^6	J^4	
			$(11, 2+\sqrt{-62})$	J^5	J^2	
			$(2,\ \sqrt{-62})$	J^4	J^7	$-\ -$
			$(11, 2-\sqrt{-62})$	J^3	J^5	
			$(7, 1-\sqrt{-62})$	J^2	J^3	
			$(3, 1+\sqrt{-62})$	J	J	
-65	$\sqrt{-65}$	$-2^2\cdot 5\cdot 13$	(1)	J^4	J^4	$+\ +\ +$
			$(3, 1-\sqrt{-65})$	J^3	J^2	
			$(9, 5-\sqrt{-65})$	J^2	AJ^2	$+\ -\ -$
			$(3, 1+\sqrt{-65})$	J	A	
			$(11, 1-\sqrt{-65})$	AJ^3	AJ^3	$-\ +\ -$
			$(2, 1+\sqrt{-65})$	AJ^2	AJ	
			$(11, 1+\sqrt{-65})$	AJ	J^3	$-\ -\ +$
			$(5,\ \sqrt{-65})$	A	J	
-66	$\sqrt{-66}$	$-2^3\cdot 3\cdot 11$	(1)	J^4	J^4	$+\ +\ +$
			$(5, 2-\sqrt{-66})$	J^3	J^2	
			$(3,\ \sqrt{-66})$	J^2	AJ^2	$+\ -\ -$
			$(5, 2+\sqrt{-66})$	J	A	
			$(7, 2+\sqrt{-66})$	AJ^3	AJ^3	$-\ +\ -$
			$(11,\ \sqrt{-66})$	AJ^2	AJ	
			$(7, 2-\sqrt{-66})$	AJ	J^3	$-\ -\ +$
			$(2,\ \sqrt{-66})$	A	J	
-67	$\frac{1+\sqrt{-67}}{2}$	-67	(1)	1	1	$+$

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakterensystem
-69	$\sqrt{-69}$	$-2^2\cdot3\cdot23$	(1)	J^4	J^4	$+\ +\ +$
			$(7, 1-\sqrt{-69})$	J^3	J^2	
			$(6, 3+\sqrt{-69})$	J^2	AJ^3	$+\ -\ -$
			$(7, 1+\sqrt{-69})$	J	AJ	
			$(5, 1+\sqrt{-69})$	AJ^3	J^3	$-\ +\ -$
			$(3, \sqrt{-69})$	AJ^2	J	
			$(5, 1-\sqrt{-69})$	AJ	AJ^2	$-\ -\ +$
			$(2, 1+\sqrt{-69})$	A	A	
-70	$\sqrt{-70}$	$-2^3\cdot5\cdot7$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+\ +\ +$
			$(7, \sqrt{-70})$	AA_1	AA_1	$+\ -\ -$
			$(5, \sqrt{-70})$	A_1	A_1	$-\ +\ -$
			$(2, \sqrt{-70})$	A	A	$-\ -\ +$
-71	$\frac{1+\sqrt{-71}}{2}$	-71	(1)	J^7	J^7	$+$
			$(2, \omega')$	J^6	J^6	
			$(5, 1+\omega')$	J^5	J^5	
			$(3, 2+\omega)$	J^4	J^4	
			$(3, 2+\omega')$	J^3	J^3	
			$(5, 1+\omega)$	J^2	J^2	
			$(2, \omega)$	J	J	
-73	$\sqrt{-73}$	$-2^2\cdot73$	(1)	J^4	J^4	$+\ +$
			$(7, 2-\sqrt{-73})$	J^3	J^2	
			$(2, 1+\sqrt{-73})$	J^2	J^3	$-\ -$
			$(7, 2+\sqrt{-73})$	J	J	
-74	$\sqrt{-74}$	$-2^3\cdot37$	(1)	J^5	J^5	$+\ +$
			$(11, 5-\sqrt{-74})$	J^4	J^4	
			$(3, 1-\sqrt{-74})$	J^3	J^3	
			$(3, 1+\sqrt{-74})$	J^2	J^2	
			$(11, 5+\sqrt{-74})$	J	J	
			$(5, 1-\sqrt{-74})$	AJ^4	AJ^4	$-\ -$
			$(6, 2+\sqrt{-74})$	AJ^3	AJ^3	
			$(6, 2-\sqrt{-74})$	AJ^2	AJ^2	
			$(5, 1+\sqrt{-74})$	AJ	AJ	
			$(2, \sqrt{-74})$	A	A	

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakteren-system
-77	$\sqrt{-77}$	$-2^2\cdot 7\cdot 11$	(1)	J^4	J^4	$+\ +\ +$
			$(3, 1-\sqrt{-77})$	J^3	J^2	
			$(14, 7+\sqrt{-77})$	J^2	AJ^3	$+\ -\ -$
			$(3, 1+\sqrt{-77})$	J	AJ	
			$(6, 1-\sqrt{-77})$	AJ^3	AJ^2	$-\ +\ -$
			$(7, \sqrt{-77})$	AJ^2	A	
			$(6, 1+\sqrt{-77})$	AJ	J^3	$-\ -\ +$
			$(2, 1+\sqrt{-77})$	A	J	
-78	$\sqrt{-78}$	$-2^3\cdot 3\cdot 13$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+\ +\ +$
			$(2, \sqrt{-78})$	AA_1	AA_1	$+\ -\ -$
			$(13, \sqrt{-78})$	A_1	A_1	$-\ +\ -$
			$(3, \sqrt{-78})$	A	A	$-\ -\ +$
-79	$\frac{1+\sqrt{-79}}{2}$	-79	(1)	J^5	J^5	$+$
			$(2, 1+\omega')$	J^4	J^4	
			$(5, \omega')$	J^3	J^3	
			$(5, \omega)$	J^2	J^2	
			$(2, 1+\omega)$	J	J	
-82	$\sqrt{-82}$	$-2^3\cdot 41$	(1)	J^4	J^4	$+\ +$
			$(7, 3-\sqrt{-82})$	J^3	J^2	
			$(2, \sqrt{-82})$	J^2	J^3	$-\ -$
			$(7, 3+\sqrt{-82})$	J	J	
-83	$\frac{1+\sqrt{-83}}{2}$	-83	(1)	J^3	J^3	$+$
			$(3, \omega')$	J^2	J^2	
			$(3, \omega)$	J	J	
-85	$\sqrt{-85}$	$-2^2\cdot 5\cdot 17$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+\ +\ +$
			$(5, \sqrt{-85})$	AA_1	AA_1	$+\ -\ -$
			$(10, 5+\sqrt{-85})$	A_1	A_1	$-\ +\ -$
			$(2, 1+\sqrt{-85})$	A	A	$-\ -\ +$
-86	$\sqrt{-86}$	$-2^3\cdot 43$	(1)	J^{10}	J^{10}	$+\ +$
			$(3, 1-\sqrt{-86})$	J^9	J^8	
			$(9, 2+\sqrt{-86})$	J^8	J^6	
			$(5, 2+\sqrt{-86})$	J^7	J^4	
			$(17, 4-\sqrt{-86})$	J^6	J^2	

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakterensystem
-86	$\sqrt{-86}$	$-2^3\cdot 43$	$(2, \sqrt{-86})$	J^5	J^9	
			$(17, 4+\sqrt{-86})$	J^4	J^7	
			$(5, 2-\sqrt{-86})$	J^3	J^5	$-\ -$
			$(9, 2-\sqrt{-86})$	J^2	J^3	
			$(3, 1+\sqrt{-86})$	J	J	
-87	$\frac{1+\sqrt{-87}}{2}$	$-3\cdot 29$	(1)	J^6	J^6	
			$(2, \omega')$	J^5	J^4	$+\ +$
			$(7, 2+\omega)$	J^4	J^2	
			$(3, 1+\omega)$	J^3	J^5	
			$(7, 2+\omega')$	J^2	J^3	$-\ -$
			$(2, \omega)$	J	J	
-89	$\sqrt{-89}$	$-2^2\cdot 89$	(1)	J^{12}	J^{12}	
			$(3, 1-\sqrt{-89})$	J^{11}	J^{10}	
			$(17, 8-\sqrt{-89})$	J^{10}	J^8	$+\ +$
			$(7, 4-\sqrt{-89})$	J^9	J^6	
			$(5, 1-\sqrt{-89})$	J^8	J^4	
			$(6, 1+\sqrt{-89})$	J^7	J^2	
			$(2, 1+\sqrt{-89})$	J^6	J^{11}	
			$(6, 1-\sqrt{-89})$	J^5	J^9	
			$(5, 1+\sqrt{-89})$	J^4	J^7	$-\ -$
			$(7, 4+\sqrt{-89})$	J^3	J^5	
			$(17, 8+\sqrt{-89})$	J^2	J^3	
			$(3, 1+\sqrt{-89})$	J	J	
-91	$\frac{1+\sqrt{-91}}{2}$	$-7\cdot 13$	(1)	A^2	A^2	$+\ +$
			$(7, \sqrt{-91})$	A	A	$-\ -$
-93	$\sqrt{-93}$	$-2^2\cdot 3\cdot 31$	(1)	$A^2A_1^2$	$A^2A_1^2$	$+\ +\ +$
			$(6, 3+\sqrt{-93})$	AA_1	AA_1	$+\ -\ -$
			$(3, \sqrt{-93})$	A_1	A_1	$-\ +\ -$
			$(2, 1+\sqrt{-93})$	A	A	$-\ -\ +$
-94	$\sqrt{-94}$	$-2^3\cdot 47$	(1)	J^8	J^8	
			$(5, 1-\sqrt{-94})$	J^7	J^6	$+\ +$
			$(7, 2-\sqrt{-94})$	J^6	J^4	
			$(11, 4+\sqrt{-94})$	J^5	J^2	

	Basis: 1, ω	d	Ideale	Klassen	Geschlechter	Charakteren-system
-94	$\sqrt{-94}$	$-2^3\cdot 47$	$(2, \sqrt{-94})$	J^4	J^7	
			$(11, 4-\sqrt{-94})$	J^3	J^5	$-\ -$
			$(7, 2+\sqrt{-94})$	J^2	J^3	
			$(5, 1+\sqrt{-94})$	J	J	
-95	$\frac{1+\sqrt{-95}}{2}$	$-5\cdot 19$	(1)	J^8	J^8	
			$(2, 1+\omega')$	J^7	J^6	$+\ +$
			$(4, 1-\omega')$	J^6	J^4	
			$(3, \omega')$	J^5	J^2	
			$(5, 1-2\omega)$	J^4	J^7	
			$(3, \omega)$	J^3	J^5	$-\ -$
			$(4, 1-\omega)$	J^2	J^3	
			$(2, 1+\omega)$	J	J	
-97	$\sqrt{-97}$	$-2^2\cdot 97$	(1)	J^4	J^4	$+\ +$
			$(7, 1-\sqrt{-97})$	J^3	J^2	
			$(2, 1+\sqrt{-97})$	J^2	J^3	$-\ -$
			$(7, 1+\sqrt{-97})$	J	J	

Reelle Körper.

	Basis: 1, ω	d	ε	$n(\varepsilon)$	Ideale	Klassen	Geschlechter	Charakterensystem
2	$\sqrt{2}$	2^3	$1+\sqrt{2}$	-1	(1)	1	1	$+$
3	$\sqrt{3}$	$3\cdot 2^2$	$2+\sqrt{3}$	$+1$	(1)	1	1	$+$
5	$\frac{1+\sqrt{5}}{2}$	5	ω	-1	(1)	1	1	$+$
6	$\sqrt{6}$	$3\cdot 2^3$	$5+2\sqrt{6}$	$+1$	(1)	1	1	$+$
7	$\sqrt{7}$	$7\cdot 2^2$	$8+3\sqrt{7}$	$+1$	(1)	1	1	$+$
10	$\sqrt{10}$	$2^3\cdot 5$	$3+\sqrt{10}$	-1	(1) $(2,\ \sqrt{10})$	A^2 A	A^2 A	$+\ +$ $-\ -$
11	$\sqrt{11}$	$11\cdot 2^2$	$10+3\sqrt{11}$	$+1$	(1)	1	1	$+$
13	$\frac{1+\sqrt{13}}{2}$	13	$1+\omega$	-1	(1)	1	1	$+$
14	$\sqrt{14}$	$7\cdot 2^3$	$15+4\sqrt{14}$	$+1$	(1)	1	1	$+$
15	$\sqrt{15}$	$3\cdot 2^2\cdot 5$	$4+\sqrt{15}$	$+1$	(1) $(2,\ 1+\sqrt{15})$	A^2 A	A^2 A	$+\ +$ $-\ -$
17	$\frac{1+\sqrt{17}}{2}$	17	$3+2\omega$	-1	(1)	1	1	$+$
19	$\sqrt{19}$	$19\cdot 2^2$	$170+39\sqrt{19}$	$+1$	(1)	1	1	$+$
21	$\frac{1+\sqrt{21}}{2}$	$3\cdot 7$	$2+\omega$	$+1$	(1)	1	1	$+$
22	$\sqrt{22}$	$11\cdot 2^3$	$197+42\sqrt{22}$	$+1$	(1)	1	1	$+$
23	$\sqrt{23}$	$23\cdot 2^2$	$24+5\sqrt{23}$	$+1$	(1)	1	1	$+$

	Basis: 1, ω	d	ε	$n(\varepsilon)$	Ideale	Klassen	Geschlechter	Charakterensystem
26	$\sqrt{26}$	$2^3 \cdot 13$	$5 + \sqrt{26}$	-1	(1)	A^2	A^2	+ +
					$(2, \sqrt{26})$	A	A	— —
29	$\frac{1+\sqrt{29}}{2}$	29	$2 + \omega$	-1	(1)	1	1	+
30	$\sqrt{30}$	$3 \cdot 2^3 \cdot 5$	$11 + 2\sqrt{30}$	$+1$	(1)	A^2	A^2	+ +
					$(2, \sqrt{30})$	A	A	— —
31	$\sqrt{31}$	$31 \cdot 2^2$	$1520 + 273\sqrt{31}$	$+1$	(1)	[illegible]	[illegible]	+
33	$\frac{1+\sqrt{33}}{2}$	$3 \cdot 11$	$19 + 8\omega$	$+1$	(1)	1	1	+
34*	$\sqrt{34}$	$2^3 \cdot 17$	$35 + 6\sqrt{34}$	$+1$	(1)	A^2	A^2	+ +
					$(3, 1 + \sqrt{34})$	A	A	— —
35	$\sqrt{35}$	$7 \cdot 2^2 \cdot 5$	$6 + \sqrt{35}$	$+1$	(1)	A^2	A^2	+ +
					$(2, 1 + \sqrt{35})$	A	A	— —
37	$\frac{1+\sqrt{37}}{2}$	37	$5 + 2\omega$	-1	(1)	1	1	+
38	$\sqrt{38}$	$19 \cdot 2^3$	$37 + 6\sqrt{38}$	$+1$	(1)	1	1	+
39	$\sqrt{39}$	$3 \cdot 2^2 \cdot 13$	$25 + 4\sqrt{39}$	$+1$	(1)	A^2	A^2	+ +
					$(2, 1 + \sqrt{39})$	A	A	— —
41	$\frac{1+\sqrt{41}}{2}$	41	$27 + 10\omega$	-1	(1)	1	1	+
42	$\sqrt{42}$	$3 \cdot 2^3 \cdot 7$	$13 + 2\sqrt{42}$	$+1$	(1)	A^2	A^2	+ +
					$(2, \sqrt{42})$	A	A	— —
43	$\sqrt{43}$	$43 \cdot 2^2$	$3482 + 531\sqrt{43}$	$+1$	(1)	1	1	+
46	$\sqrt{46}$	$23 \cdot 2^3$	$24335 + 3588\sqrt{46}$	$+1$	(1)	1	1	+
47	$\sqrt{47}$	$47 \cdot 2^2$	$48 + 7\sqrt{47}$	$+1$	(1)	1	1	+

* Die ambige Klasse A dieses Körpers enthält kein ambiges Ideal. Die ambigen Ideale $(6 + \sqrt{34})$ und $(17 - 3\sqrt{34})$ und $(\sqrt{34})$ sind alle Hauptideale.

	Basis: 1, ω	d	ε	$n(\varepsilon)$	Ideale	Klassen	Geschlechter	Charakterensystem
51	$\sqrt{51}$	$3 \cdot 2^2 \cdot 17$	$50 + 7\sqrt{51}$	$+1$	(1)	A^2	A^2	$+ \; +$
					$(3, \sqrt{51})$	A	A	$- \; -$
53	$\frac{1+\sqrt{53}}{2}$	53	$3 + \omega$	-1	(1)	1	1	$+$
55	$\sqrt{55}$	$11 \cdot 2^2 \cdot 5$	$89 + 12\sqrt{55}$	$+1$	(1)	A^2	A^2	$+ \; +$
					$(2, 1+\sqrt{55})$	A	A	$- \; -$
57	$\frac{1+\sqrt{57}}{2}$	$3 \cdot 19$	$151 + 40\omega$	$+1$	(1)	1	1	$+$
58	$\sqrt{58}$	$2^3 \cdot 29$	$99 + 13\sqrt{58}$	-1	(1)	A^2	A^2	$+ \; +$
					$(2, \sqrt{58})$	A	A	$- \; -$
59	$\sqrt{59}$	$59 \cdot 2^2$	$530 + 69\sqrt{59}$	$+1$	(1)	1	1	$+$
61	$\frac{1+\sqrt{61}}{2}$	61	$17 + 5\omega$	-1	(1)	1	1	$+$
62	$\sqrt{62}$	$31 \cdot 2^3$	$63 + 8\sqrt{62}$	$+1$	(1)	1	1	$+$
65	$\frac{1+\sqrt{65}}{2}$	$5 \cdot 13$	$7 + 2\omega$	-1	(1)	A^2	A^2	$+ \; +$
					$(5, \sqrt{65})$	A	A	$- \; -$
66	$\sqrt{66}$	$3 \cdot 2^3 \cdot 11$	$65 + 8\sqrt{66}$	$+1$	(1)	A^2	A^2	$+ \; +$
					$(3, \sqrt{66})$	A	A	$- \; -$
67	$\sqrt{67}$	$67 \cdot 2^2$	$48842 + 5967\sqrt{67}$	$+1$	(1)	1	1	$+$
69	$\frac{1+\sqrt{69}}{2}$	$3 \cdot 23$	$11 + 3\omega$	$+1$	(1)	1	1	$+$
70	$\sqrt{70}$	$7 \cdot 2^3 \cdot 5$	$251 + 30\sqrt{70}$	$+1$	(1)	A^2	A^2	$+ \; +$
					$(2, \sqrt{70})$	A	A	$- \; -$
71	$\sqrt{71}$	$71 \cdot 2^2$	$3480 + 413\sqrt{71}$	$+1$	(1)	1	1	$+$
73	$\frac{1+\sqrt{73}}{2}$	73	$943 + 250\omega$	-1	(1)	1	1	$+$
74	$\sqrt{74}$	$2^3 \cdot 37$	$43 + 5\sqrt{74}$	-1	(1)	A^2	A^2	$+ \; +$
					$(2, \sqrt{74})$	A	A	$- \; -$

	Basis: 1, ω	d	ε	$n(\varepsilon)$	Ideale	Klassen	Geschlechter	Charakterensystem
77	$\frac{1+\sqrt{77}}{2}$	$7 \cdot 11$	$4+\omega$	$+1$	(1)	1	1	$+$
78	$\sqrt{78}$	$3 \cdot 2^3 \cdot 13$	$53+6\sqrt{78}$	$+1$	(1) $(2, \sqrt{78})$	A^2 A	A^2 A	$+\ +$ $-\ -$
79	$\sqrt{79}$	$79 \cdot 2^2$	$80+9\sqrt{79}$	$+1$	(1) $(3, 1-\sqrt{79})$ $(3, 1+\sqrt{79})$	J^3 J^2 J	J^3 J^2 J	$+$
82	$\sqrt{82}$	$2^3 \cdot 41$	$9+\sqrt{82}$	-1	(1) $(3, 2-\sqrt{82})$ $(2, \sqrt{82})$ $(5, 2+\sqrt{82})$	J^4 J^3 J^2 J	J^4 J^2 J^3 J	$+\ +$ $-\ -$
83	$\sqrt{83}$	$83 \cdot 2^2$	$82+9\sqrt{83}$	$+1$	(1)	1	1	$+$
85	$\frac{1+\sqrt{85}}{2}$	$5 \cdot 17$	$4+\omega$	-1	(1) $(5, \sqrt{85})$	A^2 A	A^2 A	$+\ +$ $-\ -$
86	$\sqrt{86}$	$43 \cdot 2^3$	$10405+1122\sqrt{86}$	$+1$	(1)	1	1	$+$
87	$\sqrt{87}$	$3 \cdot 2^2 \cdot 29$	$28+3\sqrt{87}$	$+1$	(1) $(2, 1+\sqrt{87})$	A^2 A	A^2 A	$+\ +$ $-\ -$
89	$\frac{1+\sqrt{89}}{2}$	89	$447+106\,\omega$	-1	(1)	1	1	$+$
91	$\sqrt{91}$	$7 \cdot 2^2 \cdot 13$	$1574+165\sqrt{91}$	$+1$	(1) $(2, 1+\sqrt{91})$	A^2 A	A^2 A	$+\ +$ $-\ -$
93	$\frac{1+\sqrt{93}}{2}$	$3 \cdot 31$	$13+3\,\omega$	$+1$	(1)	1	1	$+$
94	$\sqrt{94}$	$47 \cdot 2^3$	$2143295+$ $221064\sqrt{94}$	$+1$	(1)	1	1	$+$
95	$\sqrt{95}$	$19 \cdot 2^2 \cdot 5$	$39+4\sqrt{95}$	$+1$	(1) $(2, 1+\sqrt{95})$	A^2 A	A^2 A	$+\ +$ $-\ -$
97	$\frac{1+\sqrt{97}}{2}$	97	$5035+1138\,\omega$	-1	(1)	1	1	$+$
101	$\frac{1+\sqrt{101}}{2}$	101	$9+2\,\omega$	-1	(1)	1	1	$+$

Register.

Die Zahlen bedeuten die Seiten des Buches.

Berichtigung.

Seite 9, Z. 14 und 15 v. o. lies: da sonst $i \equiv k$, (p) sein muß, was nicht möglich ist, weil $i - k$ seinem absoluten Betrag nach kleiner ist als p, um so mehr da $i, k \leqq p - 1$ sind.

Druck von B. G. Teubner in Leipzig.

König, Dr. **Julius**, Professor am Polytechnikum zu Budapest, Einleitung in die allgemeine Theorie der algebraischen Größen. [X u. 564 S.] gr. 8. 1903. geh. n. ℳ 18.—, in Leinwand geb. n. ℳ 20.—

Die Kroneckersche „Festschrift" vom Jahre 1881 hat der mathematischen Forschung neue Bahnen gewiesen, ja geradezu die Probleme und Ziele einer neuen Disziplin festgestellt. Diese allgemeine (algebraische und arithmetische) Theorie der algebraischen Größen versucht der Verfasser in systematischer Entwicklung vorzutragen

Durch Einführung der sogenannten „Resolventenform", die sich als weitgehende arithmetische Verallgemeinerung des Resultantenbegriffs darstellt, wurde es möglich, eine — im vollen Sinne des Wortes — allgemeine Eliminationstheorie zu schaffen, die für alle hierher gehörigen Fragen von zentraler Bedeutung ist. In durchaus ungestörter Analogie konnten die algebraischen und arithmetischen Teile der Theorie entwickelt werden, die einerseits eine „Algebra der affinen Transformationen", andererseits die „allgemeine Arithmetik" ergeben.

Kronecker, Leopold, Vorlesungen über Zahlentheorie, herausgegeben von Dr. Kurt Hensel, Professor an der Universität Marburg. In 2 Bänden. Mit Figuren im Text. I. Band. [XVI u. 509 S.] gr. 8. 1901. geh. n. ℳ 18.—

Die Herausgabe dieser Vorlesungen wurde durch den Umstand etwas verzögert, daß eine in ihnen enthaltene neue und grundlegende Untersuchung über die Zerlegung der Divisorensysteme in Faktoren von Kronecker in der unmittelbar vor seinem Tode gehaltenen Vorlesung zwar begonnen, aber nicht bis zum Ende durchgeführt worden war. Es erschien nun wünschenswert, dieses Problem, das letzte, mit welchem Kronecker sich beschäftigt hat, vollständig zu lösen und die hier sich ergebenden Resultate den Kroneckerschen Vorlesungen einzuverleiben. Zu diesem Zwecke wurde von dem Herausgeber eine Reihe eigener Untersuchungen durchgeführt, welche jetzt beendet sind, so daß die Herausgabe jener Vorlesungen nunmehr in völlig abgeschlossener Form erfolgen kann

Legendre, Adrien-Marie, Zahlentheorie. Nach der 3. Ausgabe ins Deutsche übertragen von H. Maser. 2 Bände. 2., wohlfeile Ausgabe. [I. Band: XVIII u. 442 S., II. Band: XII u. 453 S.] gr. 8. 1893. geh. n. ℳ 12.—

Einzeln: jeder Band n. ℳ 6.—

Dieses im Jahre 1830 in dritter Ausgabe unter dem Titel: „Théorie des nombres" erschienene Werk von Legendre nimmt unstreitig unter den Erzeugnissen geistiger Forschung auf mathematischem Gebiete einen sehr hervorragenden Platz ein. In eleganter, leicht verständlicher Sprache behandelt dasselbe alle bis zu jener Zeit von allen Gelehrten, vor allen aber von Legendre selbst entdeckten Eigenschaften der Zahlen. Dabei werden größere Digressionen auf verwandte Gebiete, sei es um die nötigen Hilfsmittel für die Beweisführung zu gewinnen, sei es, um die Bedeutung der Zahlentheorie für andere mathematische Disziplinen zu erweisen, nicht vermieden. In dieser Beziehung sind namentlich einerseits die Lehre von den Kettenbrüchen und die numerische Auflösung der Gleichungen, andrerseits die mit großer Ausführlichkeit im Anschluß an Gaußsche Untersuchungen behandelte Theorie der Kreisteilungsgleichungen zu erwähnen. Wenn nun auch das nur wenige Jahre nach der ersten Ausgabe des Legendreschen Werkes erschienene geniale Gaußsche Werk „Disquisitiones arithmeticae" viele der in ersterem enthaltenen Eigenschaften der Zahlen von einem höheren Gesichtspunkte aus betrachtet, wie denn überhaupt das Gaußsche Werk in methodischer Beziehung große Vorzüge vor dem Legendreschen aufweist und hierin für spätere Arbeiten maßgebend gewesen ist, so darf deshalb das Studium des letztgenannten noch nicht als überflüssig erachtet werden. Vielmehr enthält dieses Werk des Interessanten und Belehrenden noch so viel, daß dasselbe, zumal da die in ihm in Anwendung gebrachten Hilfsmittel und Methoden höchst einfacher und elementarer Natur sind, allen denen, welche sich eingehender mit der Theorie der Zahlen beschäftigen wollen, gewissermaßen zum Vorstudium für die Arbeiten von Gauß und neuerer Forscher nicht dringend genug empfohlen werden kann. Deshalb dürfte es kein unnützes Beginnen sein, dieses Werk, welches heutzutage kaum mehr oder nur nach Aufwendung bedeutender Mittel zu erhalten ist, durch eine deutsche Übersetzung wieder einem größeren Leserkreise zugänglich zu machen. Anmerkungen und Zusätze sind aber dieser Übersetzung absichtlich nicht beigefügt, noch weniger sind Änderungen innerhalb des Textes selbst vorgenommen worden.

Minkowski, Dr. **Hermann**, Professor der Mathematik an der Universität Göttingen, Geometrie der Zahlen. In 2 Lieferungen. I. Lieferung [240 S.] gr. 8. 1896. geh. n. ℳ 8.—

[Die II. Lieferung befindet sich in Vorbereitung.]

——— ——— Diophantische Approximationen. Eine Einführung in die Zahlentheorie. (Mathematische Vorlesungen an der Universität Göttingen. Bd. II.) [ca. 240 S. u. 80 Fig.] gr. 8. (Erscheint Anfang 1907.)

schließt sich einerseits die Lehre von den reellen Potenzen, Wurzeln und Logarithmen, andererseits die von den unendlichen Reihen mit reellen Gliedern. (Abschn. VII—IX.) — Nunmehr wird zur analytischen Theorie der gemeinen komplexen Zahlen übergegangen, und beim Nachweise der Behauptung, daß mit ihnen die gewöhnliche Arithmetik abgeschlossen ist, gelangen die Verfasser zum Satze von Frobenius über die Einzigkeit der gemeinen komplexen Zahlen und der Hamiltonschen Quaternionen. (Abschn. X.) — Die gemeinen komplexen Zahlen lassen sich geometrisch durch die Vektoren in der Ebene darstellen, und es entsprechen den vier Rechnungsarten mit diesen Zahlen gewisse planimetrische Konstruktionen. (Abschn. XI.) — Die trigonometrische Form ihrer Ergebnisse ist wiederum für die Arithmetik von Wichtigkeit, indem man mit Hilfe derselben die $m$ten Wurzeln aus einer gemeinen komplexen Zahl ermitteln kann. Die jetzt naheliegende Frage nach der Erklärung der Potenz für komplexe Werte der Basis und des Exponenten wird nach dem von Couchy angegebenen und von Schlömilch wirklich durchgeführten Verfahren beantwortet. (Abschn. XII.) — Den Schluß des Werkes bilden die grundlegenden Sätze über die unendlichen Reihen mit komplexen Gliedern. (Abschn. XIII.) — Vom VII. Abschnitt an kommt der Begriff der Funktion vor, nirgends jedoch der der stetigen Funktion. — Sämtliche Abschnitte mit Ausnahme des I. und V. sind mit einschlägigen Übungen versehen.

Stolz, Dr. O., weil. Professor an der Universität Innsbruck, und Dr. **J. A. Gmeiner,** Professor an der Universität Innsbruck, Einleitung in die Funktionentheorie. Zweite, umgearbeitete und vermehrte Auflage der von den Verfassern in der „Theoretischen Arithmetik" nicht berücksichtigten Abschnitte der „Vorlesungen über allgemeine Arithmetik" von O. Stolz. Mit 21 Figuren im Text. [X u. 598 S.] gr. 8. 1905. In Leinwand geb. n. *M* 15.—

Schon in der „theoretischen Arithmetik" wurde die eindeutige Funktion einer reellen Veränderlichen eingeführt und verwendet: jedoch auf die Erklärung der Stetigkeit einer solchen Funktion brauchte dort nicht eingegangen zu werden. Nunmehr tritt dieser Begriff in den Vordergrund. Dabei kann die unabhängige Veränderliche sowohl reell als auch komplex sein. Im Falle eines komplexen Argumentes gelingt es, eine Klasse von Funktionen zu bilden, wofür eine wirkliche Theorie geschaffen werden kann. Nach Weierstraß sind dies die monogenen analytischen Funktionen.

Unsere „Einleitung" zerfällt in die folgenden Abschnitte: I. Die reelle Veränderliche und ihre reellen Funktionen. II. Reelle Funktionen von zwei und mehr reellen Veränderlichen. III. Komplexe Veränderliche und Funktionen. IV. Die ganzen rationalen Funktionen. V. Die ganzen Potenzreihen. VI. Kriterien für Konvergenz und Divergenz von unendlichen Reihen. VII. Die monogene analytische Funktion einer Veränderlichen nach Weierstraß. VIII. Die Kreisfunktionen. IX. Die unendlichen Produkte. X. Die endlichen und XI die unendlichen Kettenbrüche.

Vom IV. Abschnitte an wird, soweit dies nach der Natur der Sache möglich ist, ein Unterschied zwischen reellen und komplexen Werten der Veränderlichen und Konstanten nicht mehr gemacht, wodurch eine wesentliche Vereinfachung der Darstellung erzielt wird. — Der VII. Abschnitt ist neue Zugabe zur ersten Bearbeitung der übrigen Abschnitte in den „Vorlesungen über allgemeine Arithmetik" von Stolz. Sämtliche Abschnitte sind mit zugehörigen Übungen versehen.

Veronese, Giuseppe, Professor an der Königl. Universität Padua, Grundzüge der Geometrie von mehreren Dimensionen und mehreren Arten geradliniger Einheiten in elementarer Form entwickelt. Mit Genehmigung des Verfassers nach einer neuen Bearbeitung des Originals übersetzt von Adolf Schepp, weil. Oberleutnant a. D. in Wiesbaden. Mit zahlreichen Figuren im Text. [XLVII u. 710 S.] gr. 8. 1894. geh. n. *M* 20.—

Weber, Dr. **H.,** und Dr **J. Wellstein,** Professoren in Straßburg, Encyklopädie der Elementar-Mathematik. Ein Handbuch für Lehrer und Studierende. In 3 Bänden. gr. 8. I. Band. Elementare Algebra und Analysis. Bearbeitet von H. Weber. 2. Auflage. Mit 38 Textfiguren. [XVIII u. 539 S.] 1906. In Leinwand geb. n. *M* 9.60. II. Band. Elemente der Geometrie. Bearbeitet von H. Weber, J. Wellstein und W. Jacobsthal. Mit 280 Textfiguren. [XII u. 604 S.] 1905. In Leinwand geb. n. *M* 12.— (Bd. III. Anwendungen der Elementar-Mathematik. U. d. Pr.)

Das Werk verfolgt das Ziel, den künftigen Lehrer auf einen wissenschaftlichen Standpunkt zu stellen, von dem aus er imstande ist, das, was er später zu lehren hat, tiefer zu erkennen und zu erfassen und damit den Wert dieser Lehren für die allgemeine Geistesbildung zu erhöhen. — Das Ziel dieser Arbeit ist nicht in der Vergrößerung des Umfanges der Elementar-Mathematik zu ersehen oder in der Einkleidung höherer Probleme in ein elementares Gewand, sondern in einer strengen Begründung und leicht faßlichen Darlegung der Elemente. Das Werk ist nicht sowohl für den Schüler selbst als für den Lehrer und Studierenden bestimmt, die neben jenen fundamentalen Betrachtungen auch eine für den praktischen Gebrauch nützliche, wohlgeordnete Zusammenstellung der wichtigsten Algorithmen und Probleme darin finden werden.



